RECORDS MANAGEMENT POLICY

Approval Date	October 2022
Policy Owner	Operations
Adopted by Executive Team	October 2022
Review Date	September 2024

CONTENTS

1. Introduction

1.1 The Trust recognises that by efficiently managing its records, it will be able to comply with its legal and regulatory obligations and to contribute to the effective overall management of the institution.

1.2 Records provide evidence for protecting the legal rights and interests of the Trust and provide evidence for demonstrating performance and accountability. This document provides the policy framework through which this effective management can be achieved and audited. It covers:

- Scope
- Responsibilities
- Relationships with existing policies

2. Scope of the policy

2.1 This policy applies to all records created, received or maintained by staff of the academy in the course of carrying out its functions.

2.2 Records are defined as all those documents which facilitate the business carried out by the academy and which are thereafter retained (for a set period) to provide evidence of its transactions or activities. These records may be created, received or maintained in hard copy or electronically.

2.3 A small percentage of the academy's records will be selected for permanent preservation as part of the institution's archives and for historical research. This should be done in liaison with the County Archives Service.

3. Responsibilities

3.1 The Trust has a corporate responsibility to maintain its records and record keeping systems in accordance with the regulatory environment. The person with overall responsibility for this policy is the Head of the Academy.

3.2 The School Data Protection Leads are responsible for records management in each academy and will give guidance for good records management practice and will promote compliance with this policy so that information will be retrieved easily, appropriately and in a timely way. The School Data Protection Leads will also monitor compliance with this policy by surveying at least annually to check if records are stored securely and can be accessed appropriately.

3.3 Individual staff and employees must ensure that records for which they are responsible are accurate, and are maintained and disposed of in accordance with the academy's records management guidelines. The academy follows the Information and Records Management Society (IRMS) record retention schedule found in the Records Management Toolkit for Academies in Appendix A.

4. Relationship with existing policies

4.1 This policy has been drawn up within the context of the Trust Freedom of Information Policy, Data Protection Policy and with other legislation or regulations (including audit, equal opportunities and ethics) affecting the Trust.

5. Review of policy

5.1 This policy is reviewed as required by the Trust on a bi-annual basis.

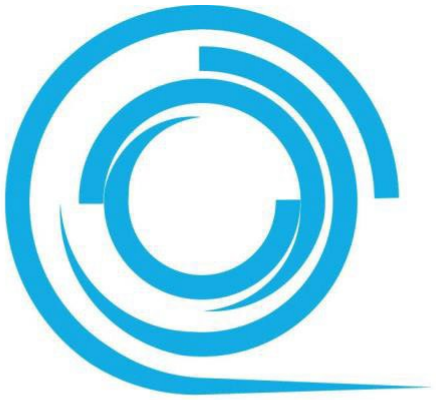
POLICY HISTORY

Policy Date	Summary of change	Contact	Implementation Date	Review Date
September 2022	New policy implemented	Operations	October 2022	September 2024

Appendix A - Records Management Toolkit for Academies

Academies Toolkit

2019



irms

the interactive hub of the information world

Association of Network Managers in Education

anme

anme Group

From the Chair - IRMS
Scott Sammons

Dear Reader,

It is my pleasure to welcome you to this brand-new Information and Records Management Toolkit for Academies Version 1.0! The Information & Records Management Society (IRMS) is a not-for-profit, volunteer-led professional membership body for the UK & Ireland. We represent and support a wide range of sectors by producing valuable and useful content like this toolkit. While this toolkit is readable free of charge to non-members, if you would like to download versions in pdf or MS Word, you can sign up to the IRMS for less than £100 a year at www.irms.org.uk/join. Signing up as a member entitles you to ask the author questions, plus a lot of other benefits. So, why not join your colleagues in the information field today, and help us fund more useful toolkits like this one?!

I am a little biased (as an Information Geek and as Chair of the IRMS), but I firmly believe in the importance and value of good information and records management practices, and this publication looks to assist in this important sector for a number of years to come. I am proud that the IRMS has been able to produce this toolkit, the third piece of our range of toolkits to support schools, charities and now academies.

If you're about to embark on reading through this toolkit and getting information handling right for your organisation, I wish you all the very best and assure you that you are in trusted hands.

This toolkit is the combination of knowledge, experience and brain wizardry of the IRMS and Kent County Council's Elizabeth Barber. My thanks also go to some key people that have been involved in the development of the toolkit: firstly, Elizabeth Barber, who has helped shape and drive the toolkit forward with such limited resources and we are forever in her debt. Secondly, Keith Batchelor, known to many in the profession, has offered his experience, expertise and time free of charge to review the content for this toolkit. My thanks also go to the wider content team for their time and input into ensuring the amazing content is up to date, reviews, and critiques to get the toolkit where it is today.

As a result, I look forward to hearing your stories of your information and records management journeys, both personally and for your organisation. May this toolkit be as useful to you as our toolkit for schools has been to many others.

All the very best,

Scott

From the Sponsor- ANME
Rick Cowell

The Association of Network Managers in Education (ANME) is a non-profit making networking company formed in 2014 by Rick Cowell, and Ben Whitaker – both Network Managers, each with over fifteen years' experience working in schools.

Why the ANME was founded:
The ANME was formed to help bring Network Managers together by getting them out of their offices, providing a venue for meeting to share best practice, network, and find colleagues in other schools facing the same issues and restraints.

In 2019, the ANME launched the Association of Data Managers in Education (ADME), the Association of Safeguarding Officers in Education (ASOE), and the Association of LGBT+ Pride in Education (ALPE).

What we do:
The ANME arranges regular meetings/conferences; inviting relevant companies to display and demonstrate their products and services, guest speakers to talk about topical issues, and providing time for networking and general discussion. Check out our website to see when the next meeting closest to you is!

We also host separate private Member portals for the ANME, ADME, and ASOE, enabling all the members to network online, seeking assistance and sharing knowledge in the privacy of their own groups.

Who is eligible to join:

ANME: Network Managers and IT Technicians employed by schools and colleges across the UK, in any sector – state, academies, free and independent.

ADME: Data Managers and Data Protection Officers employed by schools and colleges across the UK, in any sector – state, academies, free and independent.

ASOE: Safeguarding Officers and Designated Safeguarding Leads employed by schools and colleges across the UK, in any sector – state, academies, free and independent.

ALPE: All LGBT+ teachers and support staff working in schools and colleges across the UK, in any sector – state, academies, free and independent

- ✓ Free to join
- ✓ Free to attend termly meetings across the UK
- ✓ Private Member Portals
- ✓ Network with colleagues in other schools and colleges

Contents

Introduction

The Information Management Toolkit for Schools has been created to assist schools with managing their information in line with the current legislative frameworks.

Module 1 consists of the base toolkit designed to assist schools, which are under Local Authority control, in their compliance with the Freedom of Information (FoI) Act 2000.

Module 2 consists of additional information designed to assist Academies in their compliance with the FoI Act 2000 and other business requirements.

Module 3 (currently under development) will consist of additional information designed to assist independent schools with managing their records in line with legislative requirements.

This Information Management Toolkit for Academies is being made available in read-only format on the IRMS website. Members can access a pdf and MS Word version of the toolkit. Individual schools may apply for affiliate membership, which includes access to the pdf and MS Word versions of the toolkit. To find out more about this, please use the "contact us" form on the IRMS website.

All questions, suggestions and amendments to the toolkit should be sent to schooltoolkit.irms.org.uk. We will only undertake to answer questions from IRMS members, so please include your IRMS membership number when sending the question.

The Information Management Toolkit for Schools is designed as guidance and should not be quoted to users as being a "standard". All users of the toolkit should seek the advice of their own legal departments before using the toolkit. Users of the toolkit should not refer members of the public to the IRMS for clarification about the toolkit. The IRMS is not a public body, and therefore, is not subject to the FoI Act 2000. All requests for information relating to the toolkit used by individual organisations must be addressed by that organisation.

The review group consisted of the following members:

General Editor:

Elizabeth Barber Kent County Council

Contributors:

Keith Batchelor	Batchelor Associates – Records Management Consultants
Andrea Binding	Somerset County Council
Lizi Bird	Solihull Metropolitan Borough Council
Sinead Booth	Data Protection
Ciara Carroll	Cirrus Primary Academy Trust
Andy Crow	Chorus Advisers
Natalie Fear	One West, Bath and North East Somerset Council
Catrina Finch	City of Wolverhampton Council
Claire Jurczuk	Department for Education
Molly Kirkham	Gloucestershire County Council
Thomas Ng	West Berkshire Council
Romin Partnovia	Edugeek.net
Linda Shave	Institute of Information Management
Tony Sheppard	GDPR in Schools
Rebecca Taylor	Acorn Trust
Suzy Taylor	New College Durham
Alison Tennant	Liverpool Diocesan Trust
Joel Thornton	The Little IT Company

Proof-readers:

Nicola Kirwan-Williams
Dr Christopher Webb, Lambeth Palace
Scott Sammons, IRMS

Note from the Editor

The Information Management Toolkit for Academies contains a number of different fact sheets, which have been compiled by various working groups within the Review Group. This means that there is not a consistency of language or presentation across the toolkit. For example: one working group may have written in the third person where another may not. It has been decided to retain the original format of the documents as they were supplied to the editor to reflect the diversity of the working groups.

Users of the toolkit should also be aware that this guidance was compiled whilst the Independent Inquiry into Child Sexual Abuse (IICSA) was still sitting. At the time of writing, there is a moratorium on the disposal of any material which may be required by the Inquiry, and instructions have been issued to organisations explaining what they need to do. If a school is unsure about how IICSA impacts a particular group of documents, then they should seek advice from their Local Authority or legal advisers.

The Information Management Toolkit for Academies is broken up into sections. You can use the contents page above to navigate through and fine the relevant section.

Records Management Policy
Each public authority (including individual Academies) should have a records management policy. The Toolkit contains a policy document which can be adopted in its entirety or adapted to reflect the different needs of individual Academies.

- Pupil Records
- Guidelines about what should be included in the main pupil record, plus advice about what information should be transferred on to the next school/Academy, as well as how this information should be transferred.
- Records Management Programme
- The Information Management Toolkit aims to assist individual Academies with managing records throughout their life cycle.
- There is advice about managing e-mail, so as to ensure that it becomes part of the core record. There is also advice about how to conduct an information audit, along with some templates.

There is a section on managing compliance with General Data Protection Regulation (GDPR) for schools based on frequently asked questions, along with some templates. There is a section relating to the monitoring of electronic communication and the management of social media. There is also a section on information security, business continuity and digital continuity.

There are also guidelines about what needs to be considered when a school closes or changes status. There is a checklist covering requirements for physical storage areas.

Records Management Policy

Background
Section 46 of the Freedom of Information (FoI) Act 2000 requires Academies[1], as public authorities, to follow a Code of Practice on managing their records. Under section 7 of the Code of Practice on the Management of Records, it states that:

"Authorities should have in place a records management policy, either as a separate policy or as part of a wider information or knowledge management policy."

This policy needs to:

1. Be endorsed by senior management, for example: at board level, and should be readily available to staff at all levels (section 7.1).

2. Provide a mandate for the records and information management function, and a framework for supporting standards, procedures and guidelines.
   The precise contents will depend on the particular needs and culture of the authority, but it should as a minimum:
   - **a.** Set out the authority's commitment to create, keep and manage records which document its principal activities;
   - **b.** Outline the role of records management and its relationship to the authority's overall business strategy;
   - **c.** Identify and make appropriate connections to related policies, such as those dealing with e-mail, information security and data protection;
   - **d.** Define roles and responsibilities, including the responsibility of individuals to document their work in the authority's records to the extent that, and in the way that, the authority has decided their work should be documented, and to use those records appropriately;
   - **e.** Indicate how compliance with the policy and the supporting standards, procedures and guidelines will be monitored (7.2).

3. The policy should be kept up to date, so that it reflects the current needs of the authority, particularly given the rapidly changing technological environment and the embedding of the new data protection legislation. One way of ensuring this is to review it at agreed intervals, for example: annually; following an event which may require a review of practice (e.g., a subject access request); or after major organisational or technological changes, in order to assess whether it needs amendment (7.3).

4. The authority should consider publishing the policy, so that members of the public can see the basis on which it manages its records (7.4).

[For a full copy of the Lord Chancellor's Code of Practice, see http://www.nationalarchives.gov.uk/documents/information-management/foi-section-46-code-of-practice.pdf]

Having a records management policy will support the Academy in meeting its responsibilities under the Data Protection Act 2018 and the General Data Protection Regulation (GDPR).

1 Academies, by virtue of the Academies Act 2010, are subject to the Freedom of Information Act 2000. This applies to schools that have become academies since September 2010, and applies to all academies from January 2011.

Policy Template

The following extract forms part of a policy statement template which could be adopted by individual Academies. It has been extracted from a model action plan for developing records management compliant with the Lord Chancellor's Code of Practice under Section 46 of the FoI Act 2000 Model Action Plan for Schools: https://www.nationalarchives.gov.uk/documents/Schools.rtf

The policy statement template can be adopted in its entirety or can be amended to reflect the needs of individual Academies. Once it has been amended, it should be approved by the governing body or other appropriate authority. Once the records management policy has been approved at the appropriate level, it should be published, perhaps as part of the publication scheme.

[Name of Academy] Records Management Policy

The Academy recognises that, by efficiently managing its records, it will be able to comply with its legal and regulatory obligations and to contribute to the effective overall management of the institution. Records provide evidence for protecting the legal rights and interests of the Academy, and provide evidence for demonstrating performance and accountability.

This document provides the policy framework through which this effective management can be achieved and audited. It covers:

- Scope
- Responsibilities
- Relationships with existing policies

1. Scope of the policy

1.1 This policy applies to all records created, received or maintained by permanent and temporary staff of the Academy in the course of carrying out its functions. Also, by any agents, contractors, consultants or third parties acting on behalf of the Academy.

1.2 Records are defined as all those documents which facilitate the business carried out by the Academy and which are thereafter retained (for a set period) to provide evidence of its transactions or activities. These records may be created, received or maintained in hard copy or electronic format, e.g., paper documents, scanned documents, e-mails which document business activities and decisions, audio and video recordings, text messages, notes of telephone and Skype conversations, spreadsheets, MS Word documents, and presentations.

2.Responsibilities

2.1 The governing body of an Academy has a statutory responsibility to maintain the Academy records and recordkeeping systems in accordance with the regulatory environment specific to the Academy. The responsibility is usually delegated to the Head Teacher of the Academy.

2.2 The person responsible for day-to-day operational management in the Academy will give guidance on good records management practice and will promote compliance with this policy, so that information will be retrieved easily, appropriately and in a timely way. They will also monitor compliance with this policy by surveying at least annually to check if records are stored securely and can be accessed appropriately.

2.3 The Academy will manage and document its records disposal process in line with the Records Retention Schedule. This will help to ensure that it can meet FoI requests and respond to requests to access personal data under data protection legislation (subject access requests, SARS).

2.4 Individual staff and employees must ensure, with respect to records for which they are responsible, that they:

2.4.1 Manage the Academy's records consistently, in accordance with the Academy's policies and procedures

2.4.2 Properly document their actions and decisions

2.4.3 Hold personal information securely

2.4.4 Only share personal information appropriately and do not disclose it to any unauthorised third party

2.4.5 Dispose of records securely, in accordance with the Academy's Records Retention Schedule

3.Relationship with existing policies

This policy has been drawn up within the context of:

- Freedom of Information policy
- Data Protection policy
- Information Governance Policy and with other legislation or regulations (including audit, equal opportunities and ethics) affecting the Academy

Signed: [Head of Academy]

Creation and Management of School Archives

The National Archives has supplied the following information in relation to the creation and management of school archives:

If your Academy is keeping an archive (e.g., of old photographs/registers), either at your local Record Office or at your Academy, it would be right to include a statement in your Academy's Data Protection Policy to advise the public that such an archive is in place. This will help separate the personal data your Academy keeps for operational reasons and those for archive reasons and, in turn, provide a much more manageable way to deal with data subject requests. The following paragraph could be included:

The XXX Academy archive is maintained as a resource to help inspire and equip current staff and pupils to understand and appreciate issues of identity, belonging and shared heritage; to prompt memories of Academy life among many generations of Old XXXians; and to serve as a research resource for all interested in the history of XXX Academy and the community it serves.

Acknowledgements:

Content developed in 2012 by:

Anthony Sawyer	Herefordshire Public Services
John Davies	TFPL Consultancy

Reviewed in 2018 by:

Thomas Ng	West Berkshire Council
Molly Kirkham	Gloucestershire County Council
Catrina Finch	City of Wolverhampton Council

Introduction

All schools, with the exception of independent schools, are under a duty to maintain a pupil record for each pupil. Early Years settings will have their own recordkeeping requirements.

The pupil record, comprising the educational and curricula record, should be seen as the core record charting the individual pupil's progress through the education system, and should accompany them throughout their school career. This record will serve as the formal record of their academic achievements, other skills and abilities, and progress in school.

The aim of this guidance is to provide some consistency of practice in the way in which pupil records are managed across all schools. It includes suggestions on the content of the pupil record, advice on transferring to the next Academy, and retention and disposal arrangements for both paper and electronic records.

Pupil Record

Recording and disclosure of information

Pupil records may be held in paper form, or else electronically (for instance: as part of the Academy management information system (MIS)). Academies will have their own systems for maintaining pupil records, which may be a combination of electronic and hard copy files.

All information must be easy to find, accurately and objectively recorded, and expressed in a professional manner, as pupils and parents have a right of access to their educational record via the Data Protection Act 2018 and the GDPR. Requests for information by pupils, or their parents, are to be treated as subject access requests under Data Protection legislation.

Paper Files

The following information is useful on the front of a paper file, if one is held:

- Surname and forename
- Date of birth
- Unique Pupil Number
- Date file was started/opened

It may be useful to have the following information inside the front cover, so that it is easily accessible to authorised staff; this is not necessary if accessible on the school information management system:

- Emergency contact details
- Preferred name
- Names and contact details of adults who have parental responsibility/care for the pupil
- Reference to further information held on allergies/medical conditions
- Other agency involvement, e.g., Special Educational Needs (SEN), speech and language therapist
- Reference to any other linked files

Contents of the Pupil Record

The table below lists common and potential record types that may form part of the pupil record.

Record Type	Notes
Record of transfer from Early Years setting	If applicable
Admission form	
Data collection/checking form – current	This should be checked regularly by parents to ensure details are accurate
Annual written report to parents	
National curriculum and religious education locally agreed syllabus record sheets	
Any information relating to a major incident involving the child	
Statements/plans, reports, etc. for educational support, e.g., SEN, speech and language	Store in a separate area of the record or keep in a separate linked file
Medical information relevant to the child's on-going education/behaviour	Store in a separate area of the record or keep in a separate linked file
Child protection reports/disclosures and supporting documentation	Store in a separate area of the record or keep in a separate linked file, so as to limit access to specific staff
Any information relating to exclusions (fixed or permanent)	
Specific correspondence with parents or outside agencies relating to major issues	This may be in e-mail form. Once the matter is closed, save any correspondence that records sequence of events, pertinent issues and outcomes to pupil record
Summary details of complaints made by the parents or the pupil relevant to the child's on-going education/behaviour	This may be in e-mail form, see note above. Most complaints records are retained by the school and not as part of the pupil record
Examination results – pupil copy	Send uncollected certificates back to exam board after all reasonable efforts to contact the pupil have been exhausted [this is a recommendation, not a requirement]

Records Not Forming Part of the Pupil Record

The following record types should be stored separately from the main pupil record, as they are usually subject to shorter retention periods (please see the Retention Schedule section); they should not be forwarded to the pupil's next Academy:

- Attendance registers and information
- Absence (authorised) notes and correspondence
- Parental consent forms for trips/outings
- Accident forms (a copy can be placed on the pupil record if it is a major incident)
- Medicine consent and administering records (this is the school's record)
- Copies of birth certificates, passports, etc.
- Generic correspondence with parents about minor issues (i.e., 'Dear Parent')
- Pupil work, drawings, etc.
- Previous data collection forms which have been superseded (there is no need to retain these)
- Photography (image) consents (this is the school's record).

Information stored electronically

Those principles relevant to paper records will apply to those pupil records stored electronically. Academy information management systems may incorporate features to enable elements of the electronic pupil record to be deleted in accordance with retention schedules, whilst the remainder of the record remains intact.

Storage and Security

All pupil records and associated information should be stored securely to maintain confidentiality, whilst keeping information accessible to those authorised to see it. Electronic records should have appropriate security and access controls in place; equally, paper records should be kept in lockable storage areas with restricted access. Not everyone in an Academy has a need to access all of the information held about a pupil; this is particularly relevant to child protection information [see also the section on Information Security in this toolkit].

Transferring Pupil Records

It is vital to ensure swift transfers of information to the new Academy to ensure appropriate decisions can be made regarding a pupil, using relevant and accurate information.

Weeding

The pupil record should not be weeded before transfer, unless any duplicates or records with a short retention period have been included; these can be removed and securely destroyed.

Transfer Process

The following should be transferred to the next Academy within 15 school days of receipt of confirmation that a pupil is registered at another Academy:

- Common Transfer File (CTF) from the School Information Management System via the school2school system, when used
- Any elements of the pupil record, held in any format, not transferred as part of the CTF
- SEN or other support service information, including behaviour, as only limited information may be included in the CTF
- Child protection information; this must be sent as soon as possible by the Designated Safeguarding Lead (DSL) or a member of their team to their equivalent at the new Academy.

Academies must ensure the information is kept secure and traceable during transfer:

- Records can be delivered or collected in person, with signed confirmation for tracking purposes
- Pupil records should not be sent by post. If the use of post is absolutely necessary, records should be sent by 'Special Delivery Guaranteed' or via a reputable and secure courier to a pre-informed named contact, along with a list of the enclosed files. The new school should sign a copy of the list to confirm receipt of the files and securely return to the previous school
- If held electronically, records may be sent to a named contact via secure encrypted e-mail, or other secure transfer method

If the pupil is transferring to an independent school or a post-16 establishment, the existing Academy should transfer copies of relevant information only and retain the original full record as the last known Academy.

If a request is received to transfer the pupil record or other information about a pupil to a school outside of the European Union (EU), Academies should contact the Local Authority or their Data Protection Officer for further advice

Retention – Transferring Academy

Responsibility for maintaining the pupil record passes to the next Academy. Academies may wish to retain information about the pupil for a short period to allow for any queries or reports to be completed or where linked records in the Academy information management system have not yet reached the end of their retention period and deleting would cause problems.

Certain elements of the record may need to be retained for longer, for example: if litigation is pending, or for transfer to the Local Record Office, in accordance with the retention schedule.

Whilst the Independent Inquiry into Child Sexual Abuse (IICSA) is ongoing, it is an offence to destroy any records relating to the Inquiry. It is likely, at the conclusion of the inquiry, that an indication will be given regarding appropriate retention periods for child protection records. More information can be found on the IICSA website.

Academies from which a pupil transfers should consider retaining a copy of the child protection file.

Retention – Last known Academy

The last known or final Academy is responsible for retaining the pupil record. The Academy is the final or last known Academy if:

- A secondary phase and the pupil left at 16 years old or for post-16 or independent education, or;
- It is an Academy at any point and the pupil left for elective home education, they are missing from education or have left the UK.

The pupil record should be retained as a whole for 25 years from the date of birth of the pupil, after which time, if no longer required, it can be deleted or destroyed. SEN and other support service records can be retained for a longer period of 31 years to enable defence in a “failure to provide a sufficient education” case.

If a school wishes to retain data for analysis or statistical purposes, it should be done in an anonymised fashion.

Disposal

Pupil records will contain personal and confidential information and so must be destroyed securely. Electronic copies must be securely deleted, and hard copies disposed of as confidential waste. Please see the section on Safe Disposal of Records for further information.

Acknowledgements:

Original content by:

Anthony Sawyer Herefordshire Public Services
Joseph Bartoletti Middlesbrough Council

Amendments and additions made by the following as part of the 2018 review:

Lizi Bird Solihull Metropolitan Borough Council
Andrea Binding Somerset County Council
Natalie Fear One West, Bath and North East Somerset Council

1. **What is an information audit?**
An information audit is typically a record of the following:

- What information is retained
- Why information is retained
- What type of information it is
- How information is processed and shared
- Where information is stored
- What the relevant retention period is
- Who the 'responsible owners' or day-to-day users are

Note: you can expand on the audit and tailor it to your Academy, for example: you may want to combine this with data protection impact assessment (DPIA) records and information sharing agreements.

An information audit should capture all information held, regardless of its form. You should consider:

- Paper documents and records
- Electronic documents and records
- Databases (proprietary or developed in-house)
- Microfilm/microfiche
- Sound recordings
- Video/photographic records (including those records taken on traditional magnetic tape and photographic paper, but also, increasingly, digital sound, video and photo files)
- Hybrid files
- Knowledge
- Apps and portals

The information audit is designed to help organisations complete an information asset register. The terminology grows out of the concept of 'knowledge management', which involves the capture of knowledge in whatever form it is held, including encouraging people to document the information they would previously have held in their heads.

It is now generally accepted that information is an organisation's greatest asset and that it should be managed in the same way as the organisation's more tangible assets, such as staff, buildings and money.

Effective information management is about getting the right information to the right people at the right time and an information audit is key to achieving this.

2. **What are the benefits of the information audit?**

The information audit is designed to allow organisations to discover the information they are creating, holding, receiving and using, and therefore, to manage that information in order to get the most effective business use from it. For an Academy, the concept is much more concerned with accessibility of information. The information audit allows the Academy to identify the personal information it creates and stores to facilitate correct management (e.g., Record of Processing Activities) under the Data Protection Act (DPA) 2018, the General Data Protection Regulation (GDPR) and the Freedom of Information (FoI) Act 2000.

The following are all benefits to maintaining an information audit:

- It saves time – an information audit can be used as a quick point of reference for all staff; it ensures information can be easily located on a daily basis. This may also be useful for new starters or in the event of temporary cover arrangements.
- It avoids duplication – duplicating information is unnecessary, it adds to workloads and takes up unnecessary storage space, which can be costly. Duplicating personal data would be a breach of the DPA 2018, as personal data must not be excessive. Identifying where the principal copy of a piece of information is held means that individual members of staff do not need to hold their own copy.

- It helps ensure accuracy of information – having a detailed record of information improves how you manage version control, and therefore, the likelihood that you are working from the most up-to-date version.
- Compliance with the DPA – individuals have numerous rights under the DPA in relation to their personal information. Whether you are dealing with a request to access information or an erasure request, the first step is identifying whether the information is held and where. If you don't maintain a record of processing, information may be missed and you could risk Information Commissioner's Office (ICO) enforcement.

The general timescale for dealing with requests under the DPA is one calendar month. Knowing where to locate information and identify if it has been shared with third parties can help save crucial time.

- Development of a record of processing activities (RoPA) – the information collected as part of the information audit can be included in the RoPA which an Academy develops.
- It assists the Data Protection Officer – the Data Protection Officer needs an overview of what personal information is held and how it is handled.
- Compliance with the FoI Act 2000 – under the Academies Act 2010, Academies are obligated to provide certain information within 20 school days or 60 working days, whichever is shorter. Knowing what is held and where to locate information is an essential first step. Wrongly refusing a request or non-compliance with the statutory timescales could lead to ICO enforcement action.
- Identification of information which has passed its retention date – storing information can be costly, regardless of whether it is physical or electronic. Significant savings can be made by ensuring that the relevant retention periods are identified and complied with. Applying retention periods also reduces the risk of not complying with the DPA 2018, GDPR or the FoI Act 2000. Finding information and preparing it in response to a request is much more difficult if there is a need to sort through significant quantities of information which should have been disposed of.
- It improves your ability to make the right decisions – Academies deal with sensitive information on a daily basis. When making any decision in relation to the care of a child, it is essential you consider all the relevant details, whether they are medical or otherwise. You cannot complete any DPIA without knowing what information you hold or will hold.
- It reduces the possibility of an information security breach – names change, addresses change and family relationships change. Knowing where to locate the correct up-to-date information is essential. It reduces the risk of a breach, which helps prevent unnecessary distress and the likelihood of your Academy facing ICO enforcement action and/or legal claims.
- It supports accountability and transparency, which is increasingly important under GDPR requirements.

3. How to complete an information audit

The information audit works on the premise that all information is created for a purpose (business need) and the information created and stored is to support that business need. The audit works through a workflow process, identifying which information is created at which point in the process, what it is used for, for how long it is needed, whether or not it should be captured as part of the core record of the Academy (i.e., whether it is a working document or a final policy or report) and whether it needs to be protectively marked.

The information audit can be conducted in a number of ways. There are two sample templates available to download on the IRMS web pages with Module 1 of the Toolkit For Schools.

It's important that:

- you involve senior management with the audit at an early stage to ensure that they are engaged with the process and are prepared to give staff the support they need; all relevant staff are involved in the process and that they are given as much direction as possible about how to complete the audit.
- you let staff know what it is you're doing and why, even if you decide to send out templates for completion. After all, they work with the information and are best placed to identify it and any requirements. It also helps senior management and staff to understand their information responsibilities and should help ensure that the templates are completed and returned on time.
- Once this process has been completed, the information audit should contain a list of business needs, the kind of information created to meet that business need, the format in which it is stored, details on how long it needs to be kept, core records status, and any protective marking. The information audit should also contain where the information is collected from, who it is shared with, and if consent is needed and how it is obtained.
- Once the information audit has been completed, consultation with the staff actually involved in the processes needs to take place, in order to ensure that the audit is an accurate reflection of practice. At this point, some negotiation may need to take place if there are any anomalies. The purpose of the information audit is to identify where processes can be improved, not merely to document what happens at present.
- Once the information audit is felt to be accurate, then the information asset register and/or the RoPA can be agreed. This enables all members of staff to see what information is created, by which business process, where it should be filed, and how it should be managed. This helps support legal compliance and business continuity by identifying any risks and mitigations around the management of sensitive info.
- The results of the information audit should be presented to senior managers and the governing authority for comments and final approval.
- This will provide the audit with senior endorsement.

Finally, any information audit is a snapshot in time and only as good as the information provided by those taking part. In order for information systems to be kept up-to-date (including capturing information created by new and developing technologies and to take account of new functions and legislation) the audit results should be regularly reviewed and updated

Acknowledgements:

Original content developed by:

Craig Ferguson — Warwickshire County Council
Suzy Taylor — New College Durham

Keith Batchelor — Batchelor Associates

Minor amendments made at time of 2015 review.

The current version (including the template spreadsheets) was created as part of the 2018 review of the Records Management Toolkit for Schools with minor amendments to make this relevant for Academies.

Sinead Booth — Derby City Council
Catrina Finch — City of Wolverhampton

Introduction

These guidelines have been developed to provide information about electronic communications best practice and will hopefully help you balance staff and student privacy with the oversight necessary to ensure your safeguarding obligations are maintained.

The sections are:

- E-mail
- Messaging and discussion tools
- Monitoring staff and student use
- Essential resources (including relevant legislation)
- What you need to know about social media

All electronic communications, whilst they are held, are disclosable under Freedom of Information (FoI) and Data Protection legislation. Be aware that anything you write in an e-mail, an instant message (IM), a text, or on a message board could potentially be made public. Electronic communications are very easy to copy and transmit and, although you may have deleted your copy, the recipients may not. Because of this, they can form part of your records, commit you to contracts and expose your Academy to risk, if used badly.

E-mail

Watch your language
As communicating by e-mail is quick and easy, the language in which e-mail is written is often less formal and more open to misinterpretation. Use spellcheck and consider the tone of your wording.

Choose your recipients
Check the recipients are appropriate and typed correctly. Consider using role-based shared mailboxes (e.g., senco@academyname.region.sch.uk/head@academy.org.uk), ensuring you carefully control who has access to any accounts.

Consider turning off the 'auto-complete' feature in the 'To' box, as staff could easily send an e-mail to the wrong address.

Ensure that Bcc is used, where appropriate, to avoid the unauthorised disclosure of e-mail addresses of intended recipients. The Information Commissioner's Office (ICO) has taken enforcement action in cases where Bcc has not been used in sensitive cases.

Secure your data
The consequences of an e-mail containing sensitive information being sent to an unauthorised person can result in a fine of up to 20 million euros (or equivalent in sterling) or restrictions on processing from the Information Commissioner, along with adverse publicity for your Academy. Confidential or sensitive information should be sent by a secure encrypted e-mail or data transfer system. Never put personal information (such as a pupil's name) in the subject line of an e-mail.

Secure your devices
Did you know that e-mail Apps on mobile phones are usually unprotected? Did you know that, by default, Outlook will download the entire contents of a person's mailbox on a personal device (which can be easily accessed)?

If members of staff access Academy e-mails on personal devices, the Academy's IT support provider should be contacted for help with configuring the device and check for encryption, as well as ensuring that all devices require a suitable password for access. The key is to engage with your IT support provider who will be able to advise accordingly.

You could advise staff to only access work e-mail via the internet, as the web client does not save data locally.

It's not a filing system
E-mail systems are commonly used to store information which should be stored somewhere else. E-mails and attachments should be saved into any appropriate electronic filing system or printed out and placed on paper files.

Where the text of the e-mail adds to the context or value of the attached documents, it may be necessary to keep the whole e-mail. The best way to do this, and retain information which makes up the audit trail, is to save the e-mail in .msg format. Where you just want recipients to read a document, consider sending a link to the documents rather than attaching them.

How long do we keep e-mails?
E-mail is a communications tool, and e-mail applications are not designed for keeping e-mail as a record. E-mail that needs to be kept should be identified by content, for example:

- Does it form part of a pupil record?
- Is it part of a contract?
- Does it relate to an employee?

The retention for keeping these e-mails will then correspond with the types of records found in the retention schedule for Academies below. These e-mails may need to be saved into an appropriate electronic filing system or printed out and placed on paper files. Similarly, information contained within these e-mails should be recorded in the appropriate place (e.g., the management information system (MIS) or behaviour management system). Once this is done, the original could be deleted.

Consider implementing an electronic rule whereby e-mails in inboxes are automatically deleted after a period of time, assuming they have been filed away. This will assist greatly in reducing the amount of information potentially disclosable in the event that a subject access request is received.

Consider implementing procedures for the management of inboxes of staff who have left the organisation. Limiting the information which is retained will also mitigate the Academy's liability in the event of a breach and will reduce the amount of electronic storage required.

Do you want a disclaimer?
Adding a disclaimer to an e-mail mitigates risk, such as sending information to the wrong recipient. Typically, disclaimers cover the fact that information may be confidential, the intention of being solely used by the intended recipient, and that any views or opinions of the sender are not necessarily those of the Academy. There is some debate about how enforceable disclaimers are, but they can help to clarify the Academy's position in relation to the information being e-mailed.

Look out for phishing!
Make sure staff are aware of the dangers of providing information over e-mail. Never provide passwords or personal data, or click on a link in an e-mail without verifying its source. Ask your IT department to provide advice.

Messaging: Texts, instant messaging

Text messaging and IM applications provide a quick, efficient way of communicating with individuals or groups.

These methods are largely suited to brief, informal messages; more formal conversations may be better suited to e-mail, telephone or delivered face-to-face. Avoid sending and posting sensitive/personal data, as these systems may not be as secure as e-mail.

Consider your audience – it may be necessary for a message to be sent to an individual or a group of people, but bear in mind that not everyone may have access to these tools and may not have given permission for their contact details to be used in this way. It may also create privacy issues, if third parties are able to read messages not intended for them.

Internal discussion boards and forums

Internal discussion boards and forums (e.g., intranets, Microsoft Teams) provide flexibility for collaboration in the workplace. They can also be very informal and are essentially public within the organisation, although some functionality can be shared with external parties, and because of this they should never be used to share confidential or personal information.

Always ensure that staff or students that use these groups and spaces are aware of exactly who will see any information posted.

Any recorded information is subject to the same Data Protection and FoI legislation, regardless of format; therefore, it would be advisable to only use these methods of communication to transmit information which you would be content to publish, that is, low risk information due to the lack of effective security and assurance.

Records management

Content created and shared by messaging and discussion forums should be regarded as ephemeral and temporary. If the content subsequently becomes important (and is something that needs to be retained as a formal record, for example: in a safeguarding case file), then it should be copied and moved into your filing system, either by saving it in a readable electronic format, printing it out or taking a screenshot. Whilst content does exist though, it is subject to both FoI and DPA.

Monitoring staff and student use

Monitoring student and staff use of communications and the internet is a balance between an Academy's Safeguarding and PREVENT obligations and the user's right to privacy. It will be important to have a policy on this, so you can demonstrate what you intend to do and to justify this in relation to your legal obligations.

An employer can monitor the use and content of staff communications provided it has informed members of staff that it may do so. If you intend to do this, you will need to be able to prove that you have made staff aware that this may happen. You will need to have a policy and provide staff with advice on how you expect them to use systems, such as e-mail, telephone, other messaging systems and the internet (including social media).

Ensure you make a decision about how your IT provider logs people's use of your e-mail and internet, that the logging is an appropriate record, and that it suits your policy.

You should document your decisions as a retention period (see below).

Where third-party support has access to logs (remote support purposes, etc.), then you need to establish how long they, as a data processor, retain any information which may contain personal information. You should instruct the third party about the retention period based on the Academy's requirements.

The Information Commissioner's Employment Practices Code (https://ico.org.uk/media/for-organisations/documents/1064/the_employment_practices_code.pdf) is an excellent resource to use when considering this area.

Legislation

- GDPR
- DPA 2018
- FoI Act 2000
- Human Rights Act 1998
- Defamation Act 2013
- Privacy and Electronic Communications Regulations 2003
- Counter Terrorism and Security Act 2015
- Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000

Acknowledgements:

Original content developed for the 2018 revision by:

Claire Jurczuk	Department for Education
Tony Sheppard	GDPR in Schools
Suzy Taylor	New College Durham
Alison Tennant	Liverpool Diocesan Schools Trust

Minor amendments made to make the content relevant to Academies.

Social media can be used as a multi-use communication tool

Social media forms a range of versatile tools that can be used in several ways. As a communication tool, it can broadcast information, enabling a quick way to share information about the Academy in the form of text, pictures, video and/or audio. It can be used to have direct communications with stakeholders on a one-to-one, one-to-many or many-to-many basis, or it can make use of provided information to see who the Academy is engaging with.

The Academy must ensure that staff contributors maintain the Academy's standards for written communications on social media platforms. Changes to social media tools are fast-paced and it is not always possible to give consistent instructions for certain tasks. There are several organisations that can support you with understanding how to set up and make the most of social media tools, usually with a strong emphasis on the role safeguarding plays with these tools.

Use of social media may require a risk assessment prior to implementing social media; staff must think about information security when they are sending or replying to messages/posts. Use of social media should follow protocols and procedures established by the Academy to ensure consistent use of social media and that staff do not release information inappropriately or illegally.

Academies using social media will need to establish what purpose they are using it for, the lawful basis as part of it, what data/information they will process, how they will uphold any of the rights of data subjects, and the retention periods involved. This is usually completed as part of a data protection impact assessment. Depending on how the Academy is planning to use social media tools, it may opt to complete an assessment, one per tool or bring several together, based on how data flows through them (e.g., a blog post which may be tweeted and then finally published on Facebook, but is actually part of a single data flow).

Social media is not always a secure and private platform

Social media tools have a range of settings for both security and access to published posts/comments. This needs to be taken into consideration when publishing information and controlling who has access to it. Confidential or sensitive information should never be put online or shared via direct contact on social media. Where images, names of individuals or other personal data is used, Academies must ensure that they have a lawful basis for doing so.

Where this involves consent from the parents/children, the consent should be clear and unambiguous, including where the information will be shared and for how long. Records of consent should be kept with other records for the individuals involved, where possible, but access must be provided for those that require it as part of day-to-day operations. It is important for parents and students to understand that, when giving their consent, the Academy cannot control the re-posting of information.

See also:
https://www.saferinternet.org.uk/advice-centre/social-media-guides

Social media posts vary in their retention

Social media tools vary in their retention periods. When signing up for any tool, the Academy needs to ensure that users are aware of these retention periods and ensure that it checks on a regular basis for changes. Where the retention period is longer than that set out as part of standard Academy policies, processes must be in place to remove any posts or comments, or to publish this fact within the retention schedule. Where posts include items which are hard to clearly index/search (e.g., images, video or audio), then a content register may be needed to manage when items have been shared, when they were shared, who it was in reference to, etc.

Social media posts and messages don't necessarily delete immediately

Posts and messages can remain on the social media network for a period after the Academy has deleted them. Once messages have been posted they may be shared, liked and commented on (in ways not originally intended). If so, there will still be copies in existence and if the recipient saves an image/screenshot, they will have copies that can be distributed. These copies could be disclosable under the Freedom of Information (FoI) Act 2000 or under the Data Protection Act (DPA) 2018 – they will also form part of the child or subject's digital footprint, and thus, clear and unambiguous consent is therefore key.

Social media is disclosable under the access to information regimes

Both the FoI Act 2000 and DPA 2018 provide regimes for access to information based on specific requests. When completing risk assessments for publishing personal data, this must be considered as part of enabling the rights of data subjects. FoI legislation also mandates that anything published as publicly accessible is potentially disclosable

(subject to exemptions), either at the time or as part of any request.

Do staff and governors need another account for work?

In the same manner that using personal e-mail accounts for work means that they will be subject to FoI requests, the same applies for social media accounts. It is recommended, on safeguarding grounds, that dedicated work accounts are used and managed by the Academy. Any official Academy account should be tied to Academy e-mail addresses, and ensure that there is transparency within the Academy on who has access to these accounts.

Creating a social media account

Here are some steps to consider when creating a social media account. Please note that these guides are generic and are based on actions at the time of writing. Social media tools change at a fast pace and you should always check with the provider for specific guidance for use within education, or check with organisations such as the UK Safer Internet Centre or ChildNet.

Creating a Facebook account

- Go to www.facebook.com
- Enter your name, e-mail or mobile phone number, password, date of birth and gender
- Click Create an Account
- To finish creating your account, you need to confirm your e-mail

Creating a class page/group on Facebook

Facebook really has two options to use when setting up a classroom account: you can create either a page or a group.

Pages are public for everyone to see, like, and comment on. There is the capability to block specific Facebook users if there are issues, but, in general, it is a very open platform. Individuals create the page through your personal account, but that doesn't mean followers can see the creator's personal posts.

Groups can be made private or public. They can even be made 'secret', so that invitations can be sent just to the parents of a particular class. You should not send personal friend requests when setting up groups; invite them to your page with a link by copying it into an e-mail.

Creating a Twitter account

Once you are on the Twitter homepage, enter your full name, e-mail address and password to create your account. Click on Sign up for Twitter and, on the next page, Twitter will use your name as your username if it's available (if you want to change this, then do so at this stage). Click on Create My Account. Twitter will offer a few recommended accounts to follow – you can simply close this window, as my recommendation would be to only follow those Twitter accounts which make sense – and are relevant – to you. You will receive an e-mail from the Twitter verification team, click on the link in the e-mail to verify your account. Do remember to do this, as it is an important step. Once you have verified your account, you will be taken to the Twitter home page and you will be logged into your account.

Creating and sending messages/posts

Here are some steps to consider when sending messages and posting:

- Do you need to send this message/post?
- Do you need to communicate via social media, or would it be more appropriate to telephone or speak with someone face-to-face?
- Ensure that the messages/posts are clearly written
- Do not use text language or informal language in Academy messages/posts
- Always sign off with a name (and Academy contact details – never personal details)
- Make sure that you use plain English and ensure that you have made it clear how you need the recipient to respond
- Never write whole messages/posts in capital letters, as this can be interpreted as shouting
- Always spellcheck messages/posts before you send them

Sending attachments

Sending attachments on social media should be avoided; you should not be sending content to parents etc. via this platform. If they want to receive content, then they should make a request in person at the Academy or via authorised means for it to be processed. This ensures that compliance with data protection legislation is followed, as well as ensuring safeguarding issues are considered.

Broadcasting information

Where information is broadcast across social media, a record of content/audience/information may be recorded. This is both good practice for ensuring a 'draft' is clearly written and recorded, but also allows the Academy to monitor what information has been shared and about whom.

Cascading information

Where information is being re-broadcast/cascaded (e.g., a share or a RT), then it is good practice to still record this in a log. In instances where a data subject linked to the Academy has been re-broadcast, it is still affected by both FoI and DPA access regimes.

Where posts are automatically cascaded between different social networks, the security implications need to be considered to ensure that:

- Only the right level of access is in place, ensuring that personal details from one platform do not 'leak' into another platform without your permission;
- Any permissions or restrictions on sharing information on particular platforms are taken into consideration (consent records are key for this, as some data subjects may not consent to information going onto particular social media platforms), and;
- You are aware of any differences in retention periods between platforms.

Statistical information

As more Academies become media and marketing savvy, reviewing the statistics of social media tools is increasing. Generally, these hold little direct information about individuals, but where it is recorded then data minimisation principles need to apply.

Marketing

Where information is broadcast across social media in an indirect manner, it is generally accessed by those who have chosen to view and access the information. Where people have 'subscribed' to follow anything broadcast by the Academy, then a clear record of that subscription is needed. In the same way that e-mails are subject to Privacy and Electronic Communications Regulations 2003, social media tools also fall under this umbrella.

Managing your inbox

This section contains some hints and tips about how to manage incoming messages and posts. Remember that this depends on your expected use of each platform. Where you rely on any tools as part of early contact of incidents, you need to make sure it is readily monitored and is part of a range of controls you have in place.

Manage interruptions

Incoming notifications can be an irritating distraction. The following tips can help manage the interruptions:

- Turn off any alert informing you of a notification;
- Plan times to check notifications into the day;
- Only respond to posts and messages during Academy working hours. If you respond out of hours, recipients will begin to expect a reply whenever they send a message, which could cause issues and unrealistic expectations.

Manage content

Where important information is relayed to the Academy due to any incidents or early notifications from parents/stakeholders, a permanent record should be recorded in the appropriate system, including details of the original source (e.g., direct message from Twitter). This not only allows you to manage your records, but also makes access to the information more appropriate for relevant staff/individuals.

Acknowledgements:

Original content developed for the 2018 revision toolkit by:

Tony Sheppard GDPR in Schools
Becky Taylor Acorn Trust

Minor amendments made to make the content relevant to Academies.

Information Security and Business Continuity

Introduction

These guidelines have been developed to provide information on how to ensure that the Academy's management of information and records complies with your legal obligations under Data Protection law and allows you to recover your records following a security incident.

The sections are:

- Information security
- Business continuity
- Data breach management
- Essential resources and legislation

The requirement for information security within the General Data Protection Regulation (GDPR) is that the Academy's use of data must ensure "appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures".

When considering the appropriate level of security for the Academy's information and records, factors will include the risk appetite of the governing body, and any relevant policies your IT provider or governing body already has. There are tools and standards for assessing information security maturity.
These are included at the end of this guide.

Information Security

Academies must have controls in place to ensure the confidentiality, integrity and availability of the important data they process. These include:

Access controls and permissions

A policy, with associated procedures, must be in place to manage access to systems and records. This should include limits on how users access the resources, which user actions can be performed, and what resources users can access.

Records should be made of what level of access is granted and retained as part of 'new starter/change of role' records, so that access can also be correctly updated when staff leave or change roles. It should also detail who is able to authorise requests to change people's permissions.

Where individuals are given access to personal or sensitive data, additional training should be provided to ensure that they are aware of the increased risks, responsibilities (including confidentiality responsibilities), and the consequences of unauthorised access.

Staff and students must be required by the system to maintain a strong password, which must be changed as appropriate, depending on the various systems involved. Guidance is available from the Information Commissioner's Office (ICO).

Recent court and ICO decisions concerning employees' unauthorised access to sensitive information – and subsequent criminal actions in publicly posting the information – highlight the need for Academies to be able to maintain audit trails of who has access to information, as well as ensuring that appropriate security measures, including supervision, are in place.

As the Data Controller, your Academy should have data sharing agreements in place with Data Processors and/or other third parties you share data with (including Joint Data Controllers). These will include information about relevant access controls and permissions, including references to sub-Data Processors. Seek guidance from the Academy's Data Protection Officer (DPO), where appropriate.

Physical security

Physical access to records should be restricted. Key IT infrastructure, servers, certain desktop/laptop devices and paper records must be kept in restricted environments, or areas with controlled access.

Clear policies, which are readily understood by staff, must be in place to govern any removal of hard copy documents off site. Whilst the removal of hard copy documents is not to be encouraged, there may be occasions when it is necessary, in which case there should be a process for logging it.

There should also be guidelines for staff regarding locking documents in the boot of a car, if the information is to be unattended for a period of time, when they must ensure that information is kept on their person, not leaving documentation in a vehicle overnight etc.

Ideally documents should be logged as having been taken out and must be returned to Academy at the earliest possible opportunity. As with any policy, it is essential that these messages are reinforced at appropriate opportunities with all staff, beyond the point of induction.

Staff should be particularly alert to the need to shred trip packs upon return to Academy, particularly since they will contain particularly sensitive health and behavioural data of the pupils concerned.

In the Academy, filing cabinets containing personal information must be locked, as should any records storage areas. This will be paramount in the case of safeguarding records maintained by the Designated Safeguarding Lead, but it will also apply to any class records maintained by staff within the classroom.

A record of files checked out from a central system must be maintained, logging their location. Access should also be logged in the same manner/same record as for digital access to records and resources, where appropriate (e.g., pupil records archive).

A clear desk policy is the best way to avoid unauthorised access to physical records which contain sensitive or personal information – it involves the removal of physical records which contain sensitive personal information to a cupboard or drawer (lockable where appropriate). It does not mean that the desk has to be cleared of all its contents.

Documents containing personal data must be collected immediately from printers and not left on photocopiers. Academies should ideally require staff to log on to a printer or copier to obtain their prints; thus reducing the risk of data breaches. However, staff must be aware of the possibility of documents being left on the scanner area of the copier, or documents being produced in the event of a paper jam.

Where physical access cannot be fully restricted, then security measures should be taken to deal with possible removal of devices, including physical restraints (locks) and encryption.

Remote access

A remote access solution allows access to any files, databases or information systems on the network, whilst the member of staff or student is not physically located in the Academy. It should have strong security controls put in place and regular reviews to ensure that it is still secure.

Academies should decide what restrictions are necessary to prevent information or records being downloaded, transferred or printed whilst the user is off site. Devices connecting to any remote access system should be considered as part of the network and all appropriate security measures should be taken to protect the network and all systems from possible attacks from that device or any other source.

Bring your own device (BYOD)

In environments where BYOD is permitted, policies need to be in place to regulate the usage of such devices. It is best practice to ensure staff and students can't connect devices directly to the network, but have to register those devices first. Devices can be segregated from sections of the network and access to key resources better controlled and logged.

Where personal data is stored on this device (via e-mail, access to local copies of cloud storage, downloaded files, etc.) then suitable controls should be put in to place to remove it, even to the point of remotely wiping any device. Where devices cannot be remotely wiped, they should automatically wipe if repeated, unauthorised attempts to access are made. Access on devices that are not encrypted should be restricted and documents must not be stored. Access should be through secure portals and carefully controlled, with guidelines to staff being reinforced to ensure that third parties cannot gain unauthorised access to information. This includes family members in the event that shared devices are used. Devices must be password protected.

Software management

The Academy should have a policy on patching (or updating) software (including firmware) to ensure bugs are fixed and any security vulnerabilities are addressed. This should be related to the Academy's risk appetite, as patching early is generally more secure, but there is an increased likelihood of reliability issues due to bugs and potential compatibility issues. The Academy's IT provider should be able to make a recommendation based on best practice.

Anti-virus and anti-malware software require regular updates to provide appropriate protection, and this should happen in an automated fashion, with exceptions and issues notified to designated contacts. This enables key staff to be aware of any infections or risks to data within the Academy at the earliest possible opportunity; therefore, minimising risk to data. It is also recommended that you undertake a review of protection on an annual basis to ensure protection is still fit for purpose.

Software is protected by The Copyright Designs and Patents Act and gives rights of control in relation to the use and distribution of software to the software company. The licence agreement at point of purchase covers copyright and outlines how the software can be used; failure to comply with the licence and UK legislation can result in legal action.

Academies should actively engage suppliers and renew maintenance agreements to ensure that they are running the latest versions of software. More often than not, exploits (methods used by hackers to gain unauthorised access) are patched/fixed in the operating system, but outdated legacy applications are not maintained, so the threat remains. Enforcement action has been taken against organisations where breaches have occurred due to known vulnerabilities in the software and remedial action has not been taken.

Operations management

Security incidents and faults in the system can involve disclosure, alteration or loss of information, with the potential of a data breach if personal data is involved. Contingency planning for such events should form part of the Academy's critical incident management policy/business continuity planning. It is important that any incident is reported immediately to the Head Teacher and DPO, so that containment and investigation can begin (see a later section on data breaches).

The response to a security incident must include securing evidence of breaches and evidence of any weakness in existing security arrangements.

Systems management

To help understand and manage the Academy's information assets (these are usually systems in which data is held, e.g., the management information system (MIS) system, the HR and Payroll system, student files) both an information asset register (IAR) and a record of processing activity (RoPA) should be produced. It is important that an Academy knows and fully understands the information it holds and how that information is used, so that appropriate security and protection can be put in place, as per Article 30 of GDPR and steps 2–5 of the Department for Education (DfE) Data Protection Toolkit for Schools.

Organisations with 250 or more employees must document all their processing activities (RoPA). There is a limited exemption for small and medium-sized organisations that employ fewer than 250 people – they need only document processing activities that meet the following criteria:

- They are not occasional (e.g., are more than just a one-off occurrence, or something they do rarely);
- They are likely to result in a risk to the rights and freedoms of individuals (e.g., something that might be intrusive or which might adversely affect individuals);
- They involve special category data or criminal conviction and offence data (as defined by Articles 9 and 10 of the GDPR).

Within Academies, this will cover a significant number of areas and an initial review will be needed to identify what data is being used anyway.

For further information about information audits, see the appropriate section earlier in this toolkit.

For further information about IARs and retention schedules, see the relevant section later in this guide.

An Information Asset Owner (IAO) needs to be identified for each asset or group of assets. The IAO has a responsibility to ensure that the asset is managed appropriately, meets the requirements of the Academy, and monitors risks and opportunities.

Remember information assets can be hard copy files, as well as IT systems or network shares.

The ICO mentions that compiling your RoPA should not be a one-off activity and the document needs to be regularly reviewed.

Planning

The GDPR requires Academies to undertake a data protection impact assessment (DPIA) for a new project or system when the type of processing is likely to result in high risk. This could be because you're using a new technology or biometric data, or because the data is related to children. Your DPIA will help you with identifying data protection risks and will support you in demonstrating compliance with data protection laws. It is recommended that you carry out a DPIA for any new project that involves using personal data.

If the Academy's DPIA identifies a high risk that cannot be mitigated, it must consult with the ICO. To conduct a DPIA you should speak to your DPO.

When a new system is introduced, it is important to ensure that the development system, test system and associated data are kept separate from the live system and data; live data must not be used for testing or development. Where 'piloting' is needed to assess suitability, live data is frequently used, but Academies need to remember to treat the system as if it were a full system and complete any risk management activities.

The Academy also needs to ensure that they do not forget to remove data at the end of an unsuccessful 'pilot'.

For further information about GDPR, see the relevant section below.

Training

Staff, including governors and volunteers, should undergo regular training on the following:

- Data protection, including recognising what a subject access request is
- Correct use of devices and systems
- Information security
- Online safety
- Acceptable use of the Academy's IT facilities
- The Academy's procedures and protocols for sharing and disclosing personal data

Training is essential to establish a sound culture of good data protection practices. It should help to prevent data breaches and, in the event that a data breach occurs, it should help to mitigate any action taken by the ICO against the organisation. The ICO will inevitably be interested in what training employees have had when investigating any breach that is reported to it.

Network and storage management

Where Academies make use of cloud storage, instead of, or alongside, physical on-site servers, you should always ensure that the location of the cloud storage and security offered is appropriate for the information and records stored.

Appropriate client software should be available to transfer data in a secure manner, and relevant licences should ensure that the correct level of service is used, as sometimes the free version of an online service (file sharing service, survey provider) can be less secure than the business or premium version. Where files will be synced to local devices, access should, where possible, be controlled to ensure that it only syncs to agreed and encrypted devices.

Academies should try to keep data in one place, as much as possible, e.g., if Office 365 is the sharing platform, Google Drive should not be used as well.

The use of memory sticks and USB devices should be discouraged and, at a minimum, all should be encrypted.

Business Continuity

Business continuity planning includes all steps and activities required to maintain operations in the event of a disaster or disruption. It is often made up of various activities, including business impact and risk assessment, business continuity and disaster recovery.

Business impact analysis (BIA)

A BIA will enable you to identify what records are critical to the running of the Academy. You can then identify what systems and data are required to allow you to access and maintain these records. Your BIA will support you in planning the recovery of hard copy and electronic records that are critical to the operations of the Academy. Your IT provider should be able to work with you to identify critical IT systems and ensure that they are covered by effective backups.

A risk assessment should also be carried out, which will identify the threats and vulnerabilities to the records you process. You should consider how resilient your systems are, as these will be critical in ensuring the Academy can still access important data.

The Academy should identify ways to protect Academy records, in relation to the threats and vulnerabilities identified. These should focus on protecting the confidentiality, integrity and availability of your data, whether held on a computer or in paper copy.

Remember that prevention of damage to paper records must be considered. Metal filing cabinets are a good first level barrier against fire and water. Store vital records with appropriate security, not on open shelves or on the floor. Ideally, consideration should be given to transferring paper records to electronic records, where possible, with appropriate electronic backups in place.

Backup strategy

The Academy's IT provider can help to decide a suitable schedule for IT backups, based on the outcome of the BIA, giving priority to vital systems. This will also ensure they are aware of the Academy's priorities when it comes to disaster recovery.

The Academy's disaster recovery plan should focus on the restoration of records to a usable state, whether held on a server or in a filing cabinet.

The plan should include an incident response team, detailing the job roles within the Academy that are required to work together in the event of a disaster. It is important that the Academy's DPO is involved in disaster response and knows when a breach needs to be reported to the ICO.

In addition to the plans for restoring your IT systems to business as usual, you will need to consider:

Who is responsible for liaising with the incident response team?

Remember if there has been a data breach, you will need to investigate and decide whether you need to report to the ICO. If in doubt. you should contact the ICO helpdesk for advice (0303 123 1113) during office hours.

The need to ensure the Academy knows what it has lost

- How will it track down paper files that have been checked out?
- Does it have details of suppliers who may be able to recover important records that have been damaged?
- Are there any costs that might be associated with the restore? Has appropriate provision been made in the budget for this?
- Who is responsible for authorising the restoration of data? For example: the restoration of a MIS database may require multiple authorisations for the restoration to take place (i.e., both the Network Manager and the Data Manager have to agree to the restoration).

The disaster recovery plan should be tested to ensure that it can be trusted. For example: a simulation test for electronic records could involve restoring your MIS to a test environment.

Data Breach Management

As with all other organisations, Academies have had to deal with data breaches in the past and have done so with a variety of methods which haven't always been consistent. The recent changes introduced by GDPR and the Data Protection Act 2018 have consolidated what should be done and this section reviews the approach to managing records around data breaches.

There are a range of methodologies for managing breaches, how investigations take place, language used for contacting data subjects, etc. The Department for Education (DfE) has published a Data Protection Toolkit to help support Academies and the ICO has also provided advice on reporting a personal data breach, with a specific form to help organisations gather data should they need to report such a breach.

As part of data breach management, the Academy will need quick access to key records. Ensuring your DPO and any data protection leads have access to this information is essential.

All breaches should be internally logged for a number of key areas.

- Data discovered/reported to the Academy (key for starting the 72-hour countdown)
- Review of breach – what impact it had (understanding whether it is a personal data breach or not), including any commentary, category of data disclosed and number of records.
- Records of any immediate actions (to close the breach/minimise risk to individuals, if needed)
- Resultant risk and subsequent report (if risk to individuals, then report to ICO; if significant risk to individuals, then report to data subjects too)
- Subsequent actions
- Status (not a breach, not a reportable breach, reported to ICO, reported to data subjects)
- Additional actions
- Completed

The ICO form allows you to record a lot more detailed information and there are a range of toolkits and compliance engines available to hold more detailed information or guide you through actions. Updates to guidance are published via the ICO and specific Academy guidance via the DfE on a regular basis. The Academy/Trust's DPO will help the Academy decide if a breach needs to be reported to the ICO.

Records on breaches and subsequent actions will need to be retained to show how the Academy has complied with legislation. These records should be kept, according to your records retention schedules, which should specify that a record is retained until the students concerned would reach the age of 25. For data breaches relating to staff data, the retention period would be 'current year + 6 years'.

For further information about data breaches, see the section on GDPR below.

Essential Resources and Legislation

From the ICO website:

https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/security/passwords-in-online-services/

https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/data-protection-impact-assessments-dpias/when-do-we-need-to-do-a-dpia/

https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/personal-data-breaches/

From the Government:

https://www.gov.uk/government/collections/statutory-guidance-schools

https://www.ncsc.gov.uk/guidance/gdpr-security-outcomes

https://www.gov.uk/government/publications/data-protection-toolkit-for-schools

Useful Standards and Models:

ISO27000 series – Information Security
https://standards.iso.org/ittf/PubliclyAvailableStandards/c073906_ISO_IEC_27000_2018_E.zip

BS10008:2014 Evidential Weight and Legal Admissibility of Information Stored Electronically
https://shop.bsigroup.com/ProductDetail?pid=000000000030286704

ARMA GARP Maturity Model
https://en.wikipedia.org/wiki/Generally_Accepted_Recordkeeping_Principles

COBIT (IT Governance Framework)
http://www.isaca.org/cobit/pages/default.aspx

Relevant Legislation:

GDPR, Data Protection Act 2018

FoI Act 2000 Human Rights Act 1998

Privacy and Electronic Communications Regulations 2003

Copyright Designs and Patents Act 1988

Acknowledgements:

Original content for the 2018 revision of the toolkit developed by:

Romin Partnovia	EduGeek.net
Tony Sheppard	GDPR in Schools
Suzy Taylor	New College Durham
Alison Tennant	Liverpool Diocesan Schools Trust
Joel Thornton	The Little IT Company

Digital Continuity

The long-term preservation of digital records is more complex than the retention of physical records.

A large number of organisations create data in electronic format, which needs to be retained for longer than 7 years. If this data is not retained in accessible formats, the organisation will be unable to defend any legal challenge which may arise.

In order to ensure that digital records are retained in a way that ensures they can be retrieved in an accessible format when they are required, all records which are required to be retained for longer than 6 years should be part of a digital continuity statement.

The average life of a computer system can be as little as 5 years; however, as digital continuity is resource intensive, only records which are required to be retained for 6 years (in line with the Limitation Act 1980) or longer should be subject to digital continuity statements.

Purpose of digital continuity statements

A digital continuity statement will not need to be applied to all records created by the Academy. The retention schedule should indicate which records need to be subject to a digital continuity statement. Any record which needs to be preserved for longer than 6 years needs to be subject to a digital continuity statement.

Appropriate records need to be identified as early in their life cycle as possible, so that the relevant standards can be applied to them. Conversely, any records which do not need to be included in the policy should also be identified in the early part of the life cycle. Digital continuity statements should only be applied to principal copy records.

Allocation of resources

Responsibility for the management of the digital continuity strategy, including completion of the digital continuity statements, should rest with one named post holder. This will ensure that each information asset is 'vetted' for inclusion in the strategy and that resources are not allocated to records which should not be included in the strategy.

Storage of records

Where possible, records subject to a digital continuity statement should be 'archived' to dedicated server space that is being backed up regularly.

Where this is not possible, the records should be transferred to high-quality CD/DVD, if they are to be included with paper documentation in a paper file, or onto an external hard drive, which is clearly marked and stored appropriately. Records stored on these forms of storage media must be checked regularly for data degradation.

Flash drives (also known as memory sticks) must not be used to store any records which are subject to a digital continuity statement. This storage medium is prone to corruption and can be easily lost or stolen.

Storage methods should be reviewed on a regular basis to ensure that new technology and storage methods are assessed, and where appropriate added to the digital continuity policy.

Migration of electronic data

Migration of electronic data must be considered, where the data contained within the system is likely to be required for longer than the life of the system. Where possible, system specifications should state the accepted file formats for the storage of records within the system.

If data migration facilities are not included as part of the specification, then the system may have to be retained in its entirety for the whole retention period of the records it contains. This is not ideal, as it may mean that members of staff have to look on a number of different

systems to collate information on an individual or project.

Software formats should be reviewed on an annual basis to ensure usability and to avoid obsolescence.

Degradation of electronic documents

In the same way as physical records can degrade if held in the wrong environmental conditions, electronic records can degrade or become corrupted. Whilst it is relatively easy to spot if physical records are becoming unusable, it is harder to identify whether an electronic record has become corrupted, or if the storage medium is becoming unstable.

When electronic records are transferred from the main system to an external storage device, the data should be backed up and two secure copies of the data should be made.
The data on the original device and the backups should be checked periodically to ensure that it is still accessible. Additional backups of the data should be made at least once a year and more frequently, if appropriate.

Where possible, digital records should be archived within a current system. For example: a designated server where 'archived' material is stored, or designated storage areas within collaborative working tools, such as SharePoint.

Internationally recognised file formats

Records which are the subject of a digital continuity statement must be 'archived' in one of the internationally recognised file formats.

Review of digital continuity policy

The digital continuity policy should be reviewed on a biannual (or more frequently, if required) basis to ensure that the policy keeps pace with the development in technology.

Digital continuity strategy statement

Each digital continuity statement should include the following information:

- Statement of business purpose and statutory requirements for keeping records
- The statement should contain a description of the business purpose for the information asset and any statutory requirements, including the retention period for the records.

This should also include a brief description of the consequences of any data loss.

By doing this, the records owner will be able to show why and for how long the information asset needs to be kept. As digital continuity can be resource intensive, it is important that the resources are allocated to the information assets which require them.

Names of people/functions responsible for long-term data preservation

The statement should name the post holder who holds responsibility for long-term data preservation, plus the post holder responsible for the information assets. The statement should be updated whenever there is a restructure which changes where the responsibility for long-term data preservation is held.

If the responsibility is not clearly assigned, there is the danger that it may disappear, as part of a restructuring process, rather than be reassigned to a different post.

Description of the information assets to be covered by the digital preservation statement

A brief description of the information asset should be taken from the IAR.

Instructions for when the record needs to be captured into the approved file formats
The record may not need to be captured in the approved file format at its creation. For example: an MS Word document need not be converted into portable document format (pdf) until it becomes semi-current. The digital preservation statement should identify when the electronic record needs to be converted into the long-term-supported file formats identified above.
Workflow process diagrams can help to identify the appropriate places for capture.

Description of the appropriate supported file formats for long-term preservation
This should be agreed with the appropriate technical staff.

Retention of all software specification information and licence information
Where it is not possible for the data created by a bespoke computer system to be converted into supported file formats, the system itself will need to be mothballed. The statement must contain a complete system specification for the software that has been used and any licence information which will allow the system to be retained in its entirety.

If this information is not retained, it is possible that the data contained within the system may become inaccessible, with the result that the data is unusable with all the ensuing consequences.

- Description of where the information asset is to be stored
- Description of how access to the information asset is to be managed within the data security protocols

The data held for long-term preservation must be accessible when required, but also must be protected against standard information security requirements which are laid down for records within the authority. The statement must contain the policy for accessing the records and the information security requirements attached to the information assets.

Please note that this content has been included from the 2016 version of the IRMS Records Management Toolkit for Schools and has not been reviewed. The original section on Digital Continuity was created by
the Editor.

Safe Disposal of Records which Have Reached the end of Their Retention Period

Please be aware that under the terms of the Independent Inquiry into Child Sexual Abuse (IICSA) it is an offence to destroy any records that might be of relevance to the Inquiry. This overrides all business, statutory, regulatory or legal retention requirements, including data protection requirements and the data subject's right to erasure. It is anticipated that, upon conclusion of the Inquiry, further guidance regarding retention will be published.

1. Managing records retention

The fifth data protection principle states that "Personal data must be kept for no longer than is necessary for the purpose for which it is processed". Therefore, all records, in all formats, should be subject to an applicable retention period, as defined by business, statutory, regulatory, legal or historical requirements. All retention and disposal decisions should be documented in a retention schedule, as part of the Academy's records management policy (see Retention Guidelines section).

Each Academy/Trust should have an officer designated as their Academy records manager, with responsibility for ensuring records are retained, reviewed and destroyed in accordance with requirements, and as soon as possible once their lifespan has expired. The local review will determine whether records are to be selected for permanent preservation, destroyed, digitised to an electronic format, or retained for ongoing business or legal purposes.

All records in all formats must be assigned a retention period and disposal date, either upon creation or when they cease to be in active use, in accordance with the retention schedule or policy. A system should be implemented to routinely identify records, as soon as they reach their disposal date. This may form part of an electronic recordkeeping system or a manual system.

Disposal must be carried out in a timely manner to:

- Ensure compliance with business and legal retention requirements
- Improve the efficiency of the recordkeeping system
- Free up storage space
- Reduce associated storage and management costs

Destruction must include all backup and duplicate copies, in all formats. This is especially vital for personal information, which may be kept in various hybrid recordkeeping systems.

Where information is taken from one source, e.g., e-mail, and recorded in the relevant system, e.g., the behaviour management system, deletion of that e-mail which is no longer needed is not regarded as destruction of data, as the information has been moved to the correct records system. Where information is in a existing records system and is being moved to another, deletion of the original may be considered as part of data destruction.

2. Principles of disposal

Academies must agree a standard policy and procedure for the safe disposal of records. This policy must be communicated to all employees and regularly reinforced to avoid any possible data breach. Furthermore, if retention periods are not complied with, material will still have to be provided if a data subject access request or Freedom of Information (FoI) request is received.

The disposal method must be applicable to the content and format of the information. Paper and electronic records should be disposed of separately, i.e., floppy disks, CDs, DVDs, tapes, and USBs, should not be put into confidential waste containers containing paper, as they require different disposal methods and could damage shredding equipment.

Destruction must be undertaken in a way that preserves the confidentiality of the information and which makes it permanently unreadable or unable to be reconstructed or re-instated. Special care should be taken when destroying personal, sensitive or commercial information, and confidentiality should be paramount at all stages of the process.

3. Destruction of records by type

3.1 Paper records

All hard copies of official records and those containing personal data must be destroyed using confidential methods, rather than being placed in general waste bins or skips, which could result in a data breach. Specialist companies can provide confidential waste bins and other services to ensure records are disposed of in an appropriate way.

Open confidential waste bins – this method is most suited to low-level administrative records, not containing sensitive personal data, which are not governed by a business or legal retention period, and which do not require full audit trails. Bins must be placed in areas where security and access are not compromised. They must not be placed in public areas, such as reception areas. They must be clearly labelled as ‘confidential waste’, with contents being shredded on a regular basis.

- Office shredding machines – these are not usually practical, due to limited capacity and inefficient use of staff time. Ideally, they should be restricted to small ad hoc quantities and for highly sensitive and confidential documents that should be shredded immediately.
- Cross-cut or micro-shredders are preferential to strip-cut shredders, as they produce much shorter length strips, which ensures higher security levels. Controlled use of an office shredder may be the only option for Academies with limited budgets, who cannot afford to pay for a regular shredding service. A process needs to be agreed and followed in schools that are

using a shredder to ensure that information security is maintained at all times.

- Secure shredding cabinets – these are available with or without in-built shredding mechanisms. They enable records to be held safely until removed for shredding or recycling. They must be locked and placed in a secure office location, with a tamper-proof post slot and should be emptied regularly.
- Confidential waste sacks – these are available from shredding contractors. Bags must be secured (e.g., zip tied) in situ, placed in a secure area whilst awaiting collection, and a log created to identify how many bags are awaiting collection, as well as the contents of the bags.
- Shredding contractors provide the most secure method of shredding. GDPR requires that a contract be in force between the data controller (the school) and the processor (the contractor) to ensure that they both understand their obligations, responsibilities and liabilities, even if destruction is taking place on the school site.

The school will retain the responsibility of data controller, as well as the liability for non-compliance caused by the contractor under GDPR. However, if the contractor breaches the terms of the contract or acts outside of the school's instructions, it will become liable under GDPR. It is therefore essential that Academies check the terms of the contract and set out instructions in a data processing agreement on how the school's data must be handled. It is recommended that Academies check their insurance to ensure that they are not at undue risk and are adequately covered.

For example: if a contractor disposed of confidential waste inappropriately, security was breached, or data was otherwise lost whilst in the care of the contractor.

Third-party contractors should be certified to the following:

- BSEN15713 – secure destruction of confidential material
- BS7858 – staff security vetting
- ISO 9001 – service quality
- ISO 14001 – environmental management standard
- ISO 27001 – information security

Additionally, membership of the following organisations and associations are recommended:

- BSIA – British Security Industry Association
- FACT – Federation Against Copyright Theft
- FTA – Freight Transport Association
- FORS – Fleet Operator Recognition Scheme
- NAID – National Association for Information Destruction
- SafeContractor – health and safety assessment scheme
- UKSSA – UK Security Shredding Association

Third-party contractors provide a short chain of custody, which significantly reduces the risk of a data breach.

Accredited contractors will meet requirements for environmental conditions, the physical security of vehicles and facilities, and they will shred to a minimum of DIN3. Shredding contractors should be trained in the handling of confidential records. Their premises, policies, processes and accreditations should be regularly audited to ensure compliance to requirements.

Whilst contractors with accreditation may have had DBS checks, Academies should assess the level of risk in accordance with their staff supervision policies, in order to determine whether safeguarding requirements are met and whether full supervision is required.

Many contractors can provide both mobile on-site shredding and off-site shredding services. Mobile shredding services ensure that all material has left the premises shredded to approved standards. However, they also tend to

be more expensive, which means that Academies are less likely to opt for them. The chain of custody and Certificate of Destruction mean that, when an approved shredding contractor picks up the material and takes it off site, all legal responsibility transfers from the Academy to the contractor. If the Academy has completed its GDPR due diligence on the shredding contractor, off-site shredding is just as secure and possibly more economical than mobile shredding.

Approved contractors should always provide a Certificate of Destruction, which should be retained with details of individual records destroyed. A secure area must be designated where records can be stored prior to shredding.

It is vital to ensure shredded material cannot be put back together. The European standard, DIN 32757, is the standard for paper shredding. There are six levels, ranging from DIN1 to DIN6. The higher the number, the higher the standard of shredding and the smaller the shred size. DIN1–2 provide the lowest level of security; DIN5–6 are used mainly by central government and the military. DIN3–4 are recommended for public authority records, including Academy records.

3.2 Electronic and other media records

Deletion of electronic records should be a managed and auditable process, in the same manner as paper records. Records should be routinely identified for deletion and should be authorised by the relevant senior officer. Before deletion, it must be determined that all legal and business requirements have expired, and that there is no related litigation or investigation. Records must be securely deleted in accordance with the Academy's security policy. Processes must be in place to ensure that all backups and copies are included in the deletion process.

However, it is not always straightforward to delete information from electronic systems. If a system is not able to permanently and completely delete all electronic data, it should be 'put beyond use'. This means it should:

- Not be used for any decision-making, or in a manner which affects an individual in any way
- Not be given to any other organisation
- Have appropriate technical and organisational security and access controls
- Be permanently deleted when this becomes technically possible

If information is 'put beyond use', the individual's data subject access right is exempt. However, if such information is still held, it may still need to be provided in response to a court order.

The method of deletion should be suitable for the type of information. The Academy's ICT department or IT provider should be able to advise on the most appropriate method. Common methods for deleting electronic records are:

- Deletion – this is the easiest and most appropriate method for non-confidential records. However, it is important to remember that deletion from a server may not be sufficient, as this only destroys access to the record – e-discovery and recovery tools will still be able to recover the information. To achieve full destruction, overwriting with random digital code may be more appropriate.
- Overwriting – this method makes e-discovery and recovery more difficult. It is recommended to overwrite using random digital code at least three times.
- Degaussing (magnetic media) – exposing magnetic media, such as tapes and floppy disks, to a magnetic field scrambles the data beyond use or re-instatement.
- Physical destruction of the storage media – physically destroying the media on which the information is stored is the most suitable method for portable media:
- CDs/DVDs/floppy disks should be cut into pieces
- Audio/video tapes and fax rolls should be dismantled and shredded
- Hard disks should be dismantled and sanded
- USBs should be submerged in water and dismantled.

The Information Commissioner's Office (ICO) and National Cyber Security Centre (NCSC) make certain recommendations for organisations with regards to deleting,

remarking or recycling IT equipment. In accordance with this, it is recommended to use an IT asset disposal company that is fully certified with the industry body, the Asset Disposal Information Security Alliance (ADISA).

4. Transfer of information to other media

Where lengthy retention periods have been allocated to records, the Academy may wish to consider converting paper records into an alternative format, such as microfilm or digital media, e.g., scanning. The lifespan of the media, and the ability to migrate data, where necessary, should always be considered.

Consideration should also be given to the legal admissibility of records that have been converted from paper into electronic media. It is essential to have procedures in place, so that conversion is done in a standardised fashion and to ensure the quality of the electronic version. Organisations must be able to evidence that the electronic version is a genuine copy of the original, and that the integrity of the data has not been compromised.

It is recommended that original versions of records be retained for up to 6 months after transfer to an alternative medium, so as to provide adequate time in which any issues arising out of the data transfer process may be identified.

Specialist companies will transfer information to alternative media, including microfilming and scanning.

It is recommended that an external provider is used for any large-scale projects, as this is more cost-effective and has integral quality assurance standards. However, when outsourcing, it is essential to ensure that the contractor is GDPR compliant and conforms to all security and staff vetting requirements, and to have a data processing agreement in place.

Reference should be made to British Standard 10008:2008 'Evidential weight and legal admissibility of electronic information' when preparing such procedures.

Please note that scanning has been approved under IICSA, providing effective quality assurance and data integrity standards have been met, which conform to BS 10008:2008.

5. Transfer of records to the Local Record Office

Where records have been identified as being worthy of permanent preservation, arrangements should be made to transfer the records to the Local Record Office. This may be done during the records' active use, or once administrative use has concluded (depending on their condition), access requirements, and advice from the Local Record Office. Once records have been transferred, they will continue to be managed in accordance with the Data Protection Act 2018 and the FoI Act 2000 and will be subject to any applicable closure periods.

The Academy should retain details of what has been transferred to the Local Record Office to enable their identification, if required for future use.

If an Academy chooses to keep their archive records on site for use with pupils and parents, they should contact the Local Record Office for specialist advice on storage and preservation requirements.

Details of records which should be transferred to the Local Record Office can be found in the Retention Guidelines section.

6. Documenting of all archiving, destruction, deletion and digitisation of records

To satisfy audit, accountability, legal and business needs, it is vital to keep a record of all archiving, destruction, deletion and digitisation. The FoI Act 2000 requires Academies to maintain a list of records which have been destroyed and a record of who authorised their destruction.

The FoI Act 2000 states that, as a minimum, the Academy should be able to provide evidence that the destruction of records took place as part of a routine records management process. Academies must assess whether they are creating another piece of personal data by maintaining a record of evidence, particularly if they are listing the names of the people whose records have been deleted.

A comprehensive records management policy

and retention schedule will provide a detailed process to ultimately ensure that the records have been destroyed and should stand as the minimum required under the FoI Act.

A record should be retained of:

- File reference (or another unique identifier)
- File title (or brief description)
- Number of files or volumes
- Date range
- Reference to the applicable retention period
- The name of the authorising officer
- Date approved for disposal
- Date destroyed or deleted from system
- Method of disposal

- Place of disposal (whether on-site or off-site by a contractor)
- Person(s) who undertook destruction

Sample appendices are provided below for the recording of all records destroyed or deleted, transferred to the Local Record Office, or converted into an alternative medium. These records should be retained permanently by the Academy for audit purposes.

Acknowledgements:

Original contents developed by:

Sarah Graham — Information Governance Officer (Records Management) Newcastle City Council
Lia Lutfi — Birmingham City Council
Alison Marsh — Salford Royal NHS Foundation Trust

Amendments made as part of the 2018 review by:

Andrea Binding — Somerset County Council
Ciara Carroll — Cirrus Primary Academy Trust
Andy Crow — Chorus Advisers
Natalie Fear — One West, Bath and North East Somerset Council

Some minor amendments made to the section for the Academies Toolkit.

Schedule of Records Transferred by [Name of Academy]
to [Name of Organisation/Local Record Office] for Permanent Preservation

Covering Dates	Unique Identifier	Title	Description	Quantity

On behalf of the school:

Signed: .....
Name (PRINT): .....
Job Title: .....
Academy: .....
Date: .....

On behalf of the Organisation/Local Record Office:

Signed: .....
Name (PRINT): .....
Job Title: .....
Organisation: .....
Date: .....

Please return completed form to the school for permanent retention.

Proforma for individual pupil records to be converted into electronic media

Original Unique Identifier	Full Name of Pupil (SURNAME, Forename(s)	Date of Birth (DD/MM/YYYY)	Original Format of Record	New Format of Record	Date Digitised	New Unique Identifier

On behalf of the Academy:

Signed: .....
Name (PRINT): .....
Job Title: .....
Academy: .....
Date: .....

On behalf of the digitising organisation:

Signed: .....
Name (PRINT): .....
Job Title: .....
Organisation: .....
Date: .....

Destruction of original records must be undertaken and recorded in accordance with normal destruction controls and procedures. Destruction of records must be authorised by [insert appropriate person]. Original records must be retained for a period of [insert time frame of 3–6 months] before destruction. Please return completed form to the school for permanent retention.

Checklist for Storage of Physical Records

Appropriate storage for physical records

Records must be stored in the workplace in a way that does not cause a health and safety hazard. Records must not be stored in corridors or gangways and must not impede or block fire exits. There should be, where appropriate, heat/smoke detectors connected to fire alarms, a sprinkler system and the required number of fire extinguishers. The area in which records are stored should be secured against intruders and have controlled access to the working space.

Storage areas should be regularly monitored and checked for any damage or emerging risks, especially during holiday periods.

Hazards

The following are hazards which need to be considered before approving areas where physical records can be stored:

Environmental damage – fire

Records can be damaged beyond repair by fire. Smoke and water damage will also occur to records which have been in a fire, although generally records damaged by smoke or water can be repaired.

Core records should be kept in cabinets or cupboards. Metal filing cabinets will usually suffice, but, for important core records, fireproof cabinets may need to be considered.

However, fireproof cabinets are expensive and very heavy, so they should only be used in special circumstances. Core records should be identified, so that they may receive priority salvage or protection in the event of an incident affecting the storage area.

Records that are stored on desks, shelves or in cupboards which do not have doors will suffer more damage than those that are stored in cupboards/cabinets which have close-fitting doors.

Environmental damage – water

Records damaged by water can usually be repaired by a specialist document salvage company. The salvage process is expensive; therefore, records need to be protected against water damage, where possible. Where flooding is involved, the water may not always be clean and records could become contaminated as well as damaged.

Records should not be stored directly under water pipes or in places which are liable to flooding (either from excess rainfall or from the overflow of toilet cisterns). Records should be stored in cabinets/cupboards with tight-fitting doors which provide protection from water ingress. Records stored on desks or in cabinets/cupboards without close-fitting doors will suffer serious water damage.

Records should be stored at least 2 inches off the ground (most office furniture stands at this height). Portable storage containers (i.e., boxes or individual filing drawers) should be raised off the ground by at least 2 inches. This is to ensure that, in the case of a flood, records are protected against immediate flood damage.

Storage areas should be checked for possible damage after extreme weather to ensure no water ingress has occurred.

Environmental damage – sunlight

Records should not be stored in direct sunlight (e.g., in front of a window). Direct sunlight will cause records to fade and the direct heat causes paper to dry out and become brittle.

Environmental damage – high levels of humidity

Records should not be stored in areas which are subject to high levels of humidity. Excess moisture in the air can result in mould forming on the records. Mould can be a hazard to human health and will damage records, often beyond repair.

The temperature in record storage areas should not exceed 18°C and the relative humidity should be between 45% and 65%. Temperature and humidity should be regularly monitored and recorded. Storage areas should be checked for damage after extreme weather conditions to reduce the risk of mould growth.

Environmental damage – insect/rodent infestation

Records should not be stored in areas which are subject to insect infestation or which have a rodent problem (rats or mice). Frequent checks should be made to ensure that infestation has not occurred.

Disaster recovery kit

A disaster recovery kit should be at hand, for use in the event of an incident affecting the store. This should include basic equipment, such as mops, buckets and plastic sheeting, for managing a small-scale incident, as well as personal protective equipment, such as gloves and hard hats.

Cleaning

Physical storage areas should be kept clean and tidy. Rubbish should be removed and chemicals and cleaning materials also removed, or kept in designated storage cabinets, so that they do not create a fire hazard.

Electrical equipment

Use of electrical equipment within physical storage areas should be kept to a minimum, in order to reduce fire risks, with all equipment being switched off and unplugged when not in use.

The General Data Protection Regulations (GDPR)

The GDPR forms part of the data protection regime in the UK, together with the new Data Protection Act 2018 (DPA 2018). All Academies need to comply with this legislation. As part of the Government's initiative, the Department for Education (DfE) has produced a specific Data Protection Toolkit, which can be found at https://www.gov.uk/government/publications/data-protection-toolkit-for-schools.

The GDPR Section includes the following sub-sections:

- GDPR FAQs
- Data protection: Checklist
- Consent to use personal data, including:
    - Checklist for consent
    - Template Consent Form 01
    - Template Consent Form 02
- Subject Access Request Procedure
- Breach Recording

GDPR FAQs

The following FAQs are produced alongside guidance from the Information Commissioner's Office (ICO).

What information does the GDPR apply to?

The GDPR applies to 'personal data', which means any information relating to an identifiable living person that directly or indirectly identifies them, i.e., you can distinguish them from other individuals. A person's name is the most common way of identifying someone; other obviously personal data include date of birth, e-mail address and photographs of individuals.

Whether any information will identify an individual often depends on the context; a wide range of information can constitute personal data.

More than one piece of data may be necessary to identify an individual; that information may already be held, or may be available elsewhere. This means that less obvious information, such as ID numbers (e.g., pupil URN/UPN or National Insurance number, a car registration, financial details, internet protocol (IP) address, location information) can also be considered personal information.

Personal data may also include special categories. These are:

• Race
• Ethnic origin
• Political opinions
• Religious or philosophical beliefs
• Trade union membership
• Genetic data
• Biometric data (where this is used for identification purposes)
• Health data
• Sex life or sexual orientation

Special category data is considered sensitive data; you may only process them in more limited circumstances. Criminal conviction and offences data are treated in much the same way.

Personal data can be found in any format; in manual information, such as that held in structured paper files and electronic information (e.g., information stored in network files), in systems and on portable memory devices. Personal data can also be found in audio recordings and video footage, such as CCTV.

The following are instances where data is unlikely to be personal data and the requirements of GDPR are therefore unlikely to apply:

- The data is about a deceased person, although a duty of confidentiality may still exist.The data has been truly anonymised. Anonymous information has to survive the scrutiny of whoever might have access to the data; it should not be possible for someone to work out to whom the information relates. Pseudonymised data is different; it can help reduce privacy risks by making it more difficult to identify individuals, but it is still personal data.
- The data is about companies or public authorities; however, information about individuals acting as sole traders, employees, partners and company directors – where they are individually identifiable, and the information relates to them as an individual – may constitute personal data.
- The data references an identifiable individual, but does not relate to/concern them or their activities.

What should be included in my privacy notice?

The GDPR sets out the information you should supply and when individuals should be informed.

The information you supply about the processing of personal data must be:

- Concise, transparent, intelligible and easily accessible
- Written in clear and plain language, particularly if addressed to a child
- Free of charge
- Provided at the point of data collection or as soon afterwards as possible.

See the template privacy notice which is provided in the DfE Toolkit.

Are we a public authority under GDPR?

If you are a public authority, as defined under the FoI Act 2000 or FoI (Scotland) Act 2002, you will be a public authority for the purposes of the GDPR. State schools and Academies in England and Wales are public authorities.

Who is the Public Authority?

Providing the schools and academies within the MAT do not have any legal status separate from that of the MAT, the MAT is the legal entity responsible for the processing of personal data by the schools and the academies with the MAT.

The MAT would be the data controller for the processing and required to pay a data protection fee.

Do I need to appoint a data protection officer (DPO)?

Under the GDPR, you must appoint a DPO if you:

- Are a public authority;
- Carry out large-scale systematic monitoring of individuals (e.g., online behaviour tracking); or
- Carry out large-scale processing of special categories of data or data relating to criminal convictions and offences.

Therefore, Academies should appoint a DPO. Any organisation is able to appoint a DPO. Regardless of whether the GDPR obliges you to appoint a DPO, you must ensure your organisation has sufficient staff and skills to discharge your obligations under the GDPR.

You must ensure that any other tasks or duties you assign to your DPO do not result in a conflict of interest with their role as DPO.

Can organisations share a DPO?

The MAT may appoint a single DPO across all of its schools. If you wish, you may also appoint a single DPO to act for a group of Academies, taking into account their structure and size. DPO services may also be shared by being outsourced.

What are the rules on security under the GDPR?

[see also the Information Security section in this toolkit]

The GDPR requires personal data to be processed in a manner that ensures its security. This includes protection against unauthorised or unlawful processing and against accidental loss, destruction or damage. It requires that appropriate technical (such as encryption and

authentication), or organisational (such as training and implementation of policy) measures are used. Effectively, this means Academies should assess what security measures should be implemented to comply with GDPR.

What is a lawful basis for processing, and which should I use?

When processing personal data, you need a fair and lawful reason to do so. There are six available lawful bases for processing under GDPR:

1. The data subject has given clear consent for their personal information to be processed for a specific purpose
2. It is necessary for a contract you have with the data subject
3. It is necessary to comply with the law
4. It is necessary to protect someone's life
5. It is necessary to perform a task in the public interest or for official functions
6. It is necessary for your legitimate interests or the legitimate interests of a third party

No single basis is 'better' or more important than the others – whichever basis is most appropriate to use will depend on your purpose and relationship with the individual.

Most lawful bases require that processing is 'necessary'. If you can reasonably achieve the same purpose without the processing, you won't have a lawful basis.

You must determine your lawful basis before you begin processing, and you should document it. Your privacy notice should include your lawful basis for processing, as well as the purposes of the processing. Take care to get it right first time – you should not swap to a different lawful basis at a later date without good reason.

If your purposes change, you may be able to continue processing under the original lawful basis, if your new purpose is compatible with your initial purpose (unless your original lawful basis was consent).

Special category data require more protection; when using this more sensitive data, you must identify one of the six lawful bases above and, in addition, one condition from Article 9 of the GDPR. Depending on the Article 6 and Article 9 lawful bases (used in a few circumstances), you may also need to meet a condition under the DPA 2018; conditions and how they are met are listed under Part 1 and Part 2 of Schedule 1 of the act.

If you are processing criminal conviction data or data about offences, the DPA 2018 requires an additional condition to be met because Academies are not considered an 'official authority'. The conditions and how they are met are listed under Part 3 of Schedule 1 of the act.

If you are unsure about the basis for processing, then contact your DPO.

The lawful basis for your processing can also affect which rights are available to individuals.

Is parental consent always required when collecting or processing children's personal data? The GDPR contains new provisions intended to enhance the protection of children's personal data, in particular, privacy notices and parental consent for online services offered to children. Article 8 imposes conditions on children's consent, but it does not require parental consent in every case. Other lawful bases may still be available. Article 8 only applies when the controller is:

- offering Information Society Services (ISSs) directly to children and;
- wishes to rely on consent as its basis for processing.

If an ISS is only offered through an intermediary, such as a school, then it is not offered 'directly' to a child.

Academies should be mindful of any legal obligations or official duties they are required to perform as part of their core activities when considering the lawful basis, as these would not require consent as Public Authorities cannot use Legitimate Interest as a lawful basis for their core activities, but it may be appropriate for other activities, such as marketing and extracurricular clubs.

If you do wish to rely upon consent as your lawful basis for processing personal data, whether to use children's data or an adult's:

- The consent should be freely given
- The request for consent, and explanation of what the consent is for, should be concise,

easy to understand and distinct from information on other matters

- It should be easy for them to withdraw consent at any time
- The child or adult should be asked to actively opt in, because inactivity or default settings do not constitute consent
- Consent needs to be 'granular'; consent for each and every purpose should be sought

Further guidance, a checklist and templates for using consent to process personal data can be found later in this section.

What is a data breach?

A data breach is "a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of or access to personal data, transmitted, stored or otherwise processed". It can be accidental or deliberate.

How will personal data breach reporting work in practice?

Under GDPR, the reporting of personal data breaches to the ICO becomes a requirement where it is likely to result in a risk to the rights and freedoms of individuals. There is a requirement to record and possibly report the breach within 72 hours of the data controller becoming aware of the incident. Where there is high risk to the rights and freedoms of individuals, the controller is required to report the personal data breach to the data subject without undue delay, in clear and plain language. If you are not the data controller, then the most appropriate action would be to notify the data controller immediately.

Regardless of whether a breach needs to be reported to the ICO or not, breaches or potential breaches should always be recorded, contained as far as possible, mitigating action taken (if possible), and assessments made to inform any necessary changes to working practices. A log of breaches should be maintained and regularly reviewed.

Further information can be found in the DfE toolkit and also under Breach Reporting and Assessment later on in this section.

What is the data protection impact assessment (DPIA) process?

A DPIA is a tool that organisations should use to achieve good practice when bringing in new or revised processing of personal data, by identifying and minimising risks. It is effectively a risk assessment for the processing of personal information. Carrying out DPIAs is part of the Academy's accountability obligations under GDPR, and an integral part of the "data protection by default and by design" approach.

Under GDPR, a DPIA must be carried out when:

- Using new technologies
- The processing is likely to result in high risk to the rights and freedoms of individuals
- Processing is systematic and extensive, this includes profiling, and decisions that have legal – or similarly significant – effects on individuals
- Processing special categories of data, or personal data in relation to criminal convictions or offences on a large scale
- Undertaking large-scale, systematic monitoring of public areas (CCTV)

If a DPIA identifies a high risk that cannot be mitigated, the ICO must be consulted.

Does my organisation need to register under the GDPR?

The ICO provides a self-assessment tool which can be found here: https://ico.org.uk/for-organisations/data-protection-fee/self-assessment/

All schools need to register. Trusts, as the legal entity including schools, need to register on behalf of themselves and their schools. If you needed to register under the Data Protection Act 2018, then you will need to register (and pay a relevant fee) under the Data Protection (Charges and Information) Regulations 2018.

You should make a note of when any fee needs to be paid or set a date.

Does my organisation need to give the ICO details of the DPO?

Under Article 37.7 of GDPR, the Data Controller "shall publish the contact details of the data protection officer and communicate them to the supervisory authority." All Academies should inform the ICO who their DPO is.

Does my Trust register or does the Academy?

As already mentioned, the MAT/Trust is the legal entity and must register on behalf of itself and Academies within the Trust. This would include recording each Academy's details as other trading names.

Data Protection: Checklist

Action	Potential Documents
☐ We have identified different processes and activities which involve personal and/or special categories of information	Inventory of processing activities ☐ Summary record (high level) of the Academy's processing activities
☐ All levels of staff understand how the Academy will manage privacy	Data protection policy
☐ A privacy impact assessment (PIA) is completed for new processes and projects (manual or electronic)	PIA form ☐ PIA procedure/guidelines for staff PIA register (to record either results or reason for not completing a PIA)
☐ Our pupils, parents, visitors plus users of the website understand how the Academy will process their information	Privacy notice (aka fair processing notice) in plain language, covering all mandatory elements ☐ Fair processing statements on forms
☐ All staff understand how the Academy processes their information	Privacy notice for staff in plain language, covering all mandatory elements Fair processing statements on forms
☐ We have identified the processing for which we currently collect consent and have checked this is free choice	Note: Add to inventory of processing activities
☐ The way consent is collected is appropriate; sought using clear and plain language, as well as for each purpose/use of the information. Consent can easily be withdrawn at any time	Parental consent form ☐ Consent withdrawal form OR procedure for this in place Consent form, other
☐ Relevant staff understand how to process a request to access personal information (subject access request (SAR)), the right to objection and the right to erasure, and it is easy for individuals to make a request	SAR procedure ☐ Request form – optional, but may make it easier to deal with requests because you will have a clearer picture of what the individual wants Record of disclosure – retain in case of queries or repeat requests
☐ We have reviewed how information is accessed at the Academy, by whom and have checked this is appropriate	Documentation managing access rights to systems and network drives and consideration of how physical/paper information is stored and accessed

Guidance on Consent to Use Personal Data

When processing personal data, organisations need a fair and lawful reason to do so. Most public sector organisations process personal data to complete a task carried out in the public interest or in the exercise of official authority, but, if this is not the case, sometimes the consent of an individual has to be relied upon.

What is consent?

Consent is one of six lawful bases to process personal data. 'Consent' under the GDPR has a particular meaning; it should always be freely given, specific, informed and an unambiguous indication of an individual's wishes with regard to the processing of their personal data.

When to use consent

Consent to use an individual's personal data should only be sought if you can offer genuine choice and control over how their data is used. An example of an appropriate time to collect consent in an Academy or Academy setting is asking for consent to use a photograph in an Academy newsletter, website, etc.; pupils/parents can refuse consent in this instance without any detriment, such as being denied an education or other services.

When not to use consent

If a genuine choice cannot be offered, consent is not appropriate and should not be used. If the personal data would still be used without consent, asking for it is misleading and unfair. This could destroy trust, damage reputation and could lead to enforcement action being taken by the ICO. Collecting consent would be unfair where there is any element of compulsion or pressure. It should be separate from other terms and conditions and should not be a precondition of service provision. Public authorities, including Academies, employers and other organisations in a position of 'power', may find it more difficult to show freely given consent.

If consent is not appropriate as a basis for processing, another lawful basis for processing must be identified. If another lawful basis cannot be found, then processing should not take place.

How to obtain and record consent

A request for consent, and the explanation of what the consent is to be used for, should be concise, easy to understand and distinct from information on other matters. The following information is the minimum to be provided when seeking consent to use personal data:

- Name of the organisation
- Purpose for each use of the data for which consent is sought
- Type of data that will be used
- Details of the right to withdraw consent at any time and how this can be done
- Details of any third parties who will also use the data and why
- If applicable, the location and possible risks of transfers to countries outside of the EU.

Individuals should be asked to actively opt in – silence, inactivity, pre-ticked boxes or other default settings do not constitute consent.

GDPR also requires 'granular' consent for each and every purpose for which data is to be processed. Individuals should be free to choose which purpose or purposes they accept, rather than having to consent to a bundle of purposes or none at all. Returning to the earlier example on consent to use a photograph in the Academy, displaying a child's photo in the classroom is very different in purpose and use to adding a photo of a child to the Academy website.

Consent can be collected in a number of ways, including the signing of a form with tick boxes, ticking a box when visiting a website, or by any other action which clearly indicates an individual's choice. However, it is collected, a clear record which demonstrates consent has been obtained needs to be kept. The burden of proof is on the collecting organisation.

Withdrawal of consent

The GDPR gives a specific right to withdraw consent. Organisations need to tell individuals about their right to withdraw at any time, and make it as easy to withdraw their consent as it was to provide it.

Is consent that was provided pre-GDPR still valid?

There is no set time limit for the validity of consent. How long it lasts will depend on context, potential risks to the privacy of the individual and how likely it is that circumstances may change.

If consent was provided before GDPR was enacted, it will be important to apply the principles of the checklist below to ensure that it is valid and was documented. Check whether existing consents are appropriate and review the way consent is collected. If existing mechanisms comply with GDPR, there is no need to obtain fresh consent.

See below for a consent checklist and a template form.

Checklist for consent

This checklist is adapted from the guidance provided by the ICO.

Asking for consent

- ☐ We have checked that consent is the most appropriate lawful basis for processing
- ☐ We have made the request for consent separate from other matters
- ☐ We ask individuals to positively opt in
- ☐ We don't use pre-ticked boxes or any other type of default consent
- ☐ We use clear, plain language that is easy to understand
- ☐ We tell individuals who we are
- ☐ We specify why we want the data and what we're going to do with it
- ☐ We give the option to consent separately to different purposes and types of processing
- ☐ We name any third-party controllers who will be relying on the consent
- ☐ We tell individuals that they can withdraw their consent
- ☐ We ensure that individuals can refuse to consent without detriment
- ☐ We avoid making consent a precondition of a service

Recording consent

- ☐ We keep a record of when and how we got consent from the individual
- ☐ We keep a record of exactly what they were told at the time

Managing consent

- ☐ We regularly review use of consent
- ☐ We have processes in place to refresh consent at intervals appropriate to the context
- ☐ We have procedures in place to allow consent preferences to be checked and managed
- ☐ We make it easy for individuals to withdraw their consent at any time, and inform them how to do so
- ☐ We act on withdrawals of consent as soon as we can
- ☐ We don't penalise individuals who wish to withdraw consent.

Template Consent Form for Academies 01

Instructions for use: The text below can be transferred onto your Academy's headed paper. Read through to make sure it is relevant to your Academy and how you will use the photos/videos. Text in [square brackets] is an instruction or needs to be replaced with your Academy's information. Text should only be used if relevant, and can be deleted if it is not relevant. This template can also be adapted for other forms used to record consent for pupil's personal data, e.g., creation of profiles on external/online software, if consent is necessary.

[INSERT name of Academy]
Consent for Children to Appear in Photographs or in Videos and How They Will Be Used

We occasionally take photographs of the children at our Academy. These images may be used in [INSERT HOW YOU WILL USE, e.g., our Academy prospectus, in other printed publications that we produce, on our Academy website, on project display boards in Academy]. We may also make video or webcam recordings for [INSERT HOW YOU WILL USE, e.g., Academy-to-Academy conferences, examinations and coursework].

It is important that we protect your child's interests, respect your wishes and comply with Data Protection law. Please read the Conditions of Use below before answering the questions below and signing and dating this form. Please return the completed form (one for each child) to the Academy as soon as possible; we will not use a photograph or video of your child without consent.

Please note there are certain activities where we do not use consent as the basis for processing your child's data. There are described in our Privacy Notices [INSERT WHERE AVAILABLE, e.g., website link]. We may also take photos/video of your child for identification purposes and for evidencing their educational development – such data will sit on their file and not be shared, unless the law requires us to do so or you have given your specific consent.

Where your child is over 13 years of age, we recommend that you complete this form with them, as children may be able to decide how their data may be used in certain circumstances.

Please note that you can withdraw your consent at any time. If you have any queries or wish to withdraw or review your consent, you can contact [INSERT Academy Lead/Data Protection Officer]

Conditions of Use:

This form is valid [INSERT TIME VALID FOR, e.g., for the period of one academic year]. Your consent will automatically expire after this time.

The Academy will not re-use any photographs or recordings of your child that are incompatible with the original purposes explained to you.

If we use photographs of individual pupils, we will not use the full name of that child in any accompanying text or caption without consent, nor will we include any other personal data.

We may use group or class photographs or footage with very general labels, such as 'a science lesson'.

Description of event: [INSERT description here]
Purposes for which the [DELETE AS APPROPRIATE photograph/video/child's name] will be used: [INSERT purpose here]
Description of coverage: [INSERT names of newspapers/TV channels and any other relevant details]

May we allow your child to appear in the media coverage as described above? Please note: once a photograph appears in the media, the Academy has no control over who else may use the images/storyline	Yes ☐	No ☐

I have read and understand the conditions of use attached to this form.

Name of Child .....

Name of Parent/Carer .....

Signed (Parent/Carer) Dated:

Subject Access Request (SAR) Procedure

This is a suggested procedure for Academies to follow, in order to help them process a SAR appropriately and within the required timescales. A template SAR form has also been provided for Academies to adapt should they wish, but they are not mandatory.

Receiving a SAR

A SAR is received from a pupil, parent, member of staff or other individual for whom the Academy holds information. This may be received either verbally, in writing or via a form (see example template below) which is made available on the website or from the Academy office.

Pass the SAR to the DPO or person responsible for processing SARs, who will acknowledge receipt of the request.

If the request is in writing or via a form, ensure it is clear what the individual wants. If the request is received verbally, it may be appropriate to seek clarification from the requestor to ensure the correct information is sought for them. Seek confirmation of the information the individual would like if it is not clear.

Check identity and authorisation

Ask the requestor to provide evidence of their identity in the form of a current passport/driving license. This may not be necessary if the requestor is known and you are sure they are who they say they are.

Keep a record of the identification checks that were conducted.

A copy of identification used is not required.

If the requestor is making a SAR on behalf of a pupil or other individual, ensure that they have the authority to do so. For example: a request can be made by a solicitor or by a parent on behalf of their child where they have parental responsibility or they have care of the child; however, individual circumstances should be considered.

If the child is deemed to be competent to make their own request (usually only relevant in secondary settings), then the information should be released to them or their consent sought.

Collect and prepare the data

Collect the data requested. This may require searching across multiple filing systems, formats and systems/databases in the Academy, as well as archived files, e-mail folders and archives.

Don't provide original documents to the requestor; instead, make copies of documents, or copy and extract the relevant data.

Review the data to identify whether any third-party data are present in it, and either redact the identifying third-party information from the documentation – this may not just be limited to a name, other information may identify them – or obtain written consent from the third party for their identity and personal data to be revealed. In practice, staff names will generally remain (where acting in their professional capacity), but the data and names of pupils and parents will need to be redacted.

Supply the data

Consider how you will supply the requestor with the data and whether any security precautions should be taken (such as confirming the address, sending special delivery or handing directly to them).

Meet the legal requirement to provide the requested data to the requestor within one calendar month from the date on which the request was received. A further 2 months can

be taken to respond if the request is of a particularly complex nature; however, the requestor should be made aware of this as soon as possible.

Keep a record

On a SAR log maintain a record of requests for data, receipt of the data, and relevant dates.

It is useful to retain a copy, for a short period, of the data provided, as well as any information withheld. This is so that queries or a request for a review can be responded to.

Template SAR Form

Academy Data Subject Access Request Form

If you wish to make a request for personal data under Data Protection legislation, please complete the form below to enable us to meet your request. The form is not mandatory; however, it will help us to respond to your request as quickly as possible. The Academy will endeavour to respond to your request within one calendar month. We may extend this time if the request is complex; however, we will inform you of this within one month of receipt of the request, together with the reason(s) for delay.

The form can be submitted to the Academy via e-mail to [INSERT contact e-mail] or by posting to [INSERT contact and address].

Your name:		**E-mail or postal address: (whichever is your preferred contact meth od)**		
Phone number: (optional – - used to con tact you about request)				
Are you the Data Subject?	Yes ☐	No ☐	**If you selected 'No', add name of Data Subject:**	
Your relationship to the Data Subject, or state 'Not applicable':				
If you are requesting data on behalf of a child, please note that we may consult with the child, if we believe that they have the capacity to understand this request.				
Do you want a copy of some personal data?	Yes ☐	No ☐	If No, please select another option below:	
Information about processing ☐	Correction of data ☐	Erasure of data ☐	Objection to/ ☐	Restrict use of data
If Yes, what data? Please describe below and provide as much detail as possible to aid us in our search				
Have you enclosed/attached a copy of your photo ID?	Yes ☐	No ☐		
Please sign:		**Date:**		

Breach Recording

[For additional information about breach recording, see also the Information Security section of this toolkit.]

A personal data breach is defined as "a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed."

Under the GDPR, breaches which are "unlikely to result in a risk to the rights and freedoms of natural persons" do not require notification to the ICO. Where reporting is required, it should be done within 72 hours of discovery.

Regardless of whether a breach needs to be reported to the ICO, breaches or potential breaches should always be recorded, mitigating action taken (if possible), and assessed to inform whether or not any changes to working practices are required. In making the assessment, the Academy should consider the likely impact on data subjects, including:

- Physical threat to safety
- Discrimination
- Identity theft or fraud
- Financial loss
- Damage to reputation
- Loss of confidentiality
- Any other significant economic or social disadvantage to the individual(s) concerned

When the personal data breach is likely to result in a high risk to the rights and freedoms of affected individuals, those impacted should be informed without undue delay. Informing people and organisations that have experienced an incident can be an important element in helping to manage the situation; for example: notifying an individual whose information was misdirected would help them take to precautions against ID theft, fraud etc.

However, if notification would serve only to worry the person concerned without any benefit, it may not be appropriate[2].

Notification should have a clear purpose.
The purpose of the Breach Recording and Assessment form is to:

- Provide a consistent approach to responding to information security breaches
- Determine whether the ICO should be notified about the incident
- Provide an overview of the incident for the Head Teacher/governance structure at Trust level, along with recommendations on what action should be taken to address matters and to prevent a reoccurrence

Further information can be found in the DfE toolkit.

The assessment form will support an Academy in considering:
- Containment
- Level of risk
- Notification
- Evaluation and response

[2] Art. 34.3 only covers where data is unintelligible, where measures have already been taken to deal with the impact, or when a public comms plan is needed instead.

Template Breach Recording Form

[INSERT name of Academy] Record of Data Protection Breach

Name of Data Protection Officer:
ICO registration number:

Completed by (Name):	
Job title:	
Contact e-mail address and phone number:	
Date breach occurred:	
Date breach discovered:	
Date breach reported:	
Date investigation started:	
Date investigation completed:	
Description and nature of the breach:	
Number of Data Subjects involved:	
Volume of personal data:	
Category of personal data: *List the broad types of information*	
Further details of the personal data:	
Containment action: *Summarise actions taken to recover from the mistake, measures taken to mitigate any possible adverse effects on the individual(s) concerned and actions taken to stop it getting worse, e.g., 'collected information', or 'asked recipient to delete it'.*	
Risks as a result of the breach: *Describe the risks or consequences; for example: if the information contained financial data, such as bank account numbers, then there may be a risk of fraud, or if the information contained sensitive health and personal data, then there may be a safeguarding issue that could leave the affected individual vulnerable.*	
Overall impact of the breach: *Consider: Sensitivity of the data, volume of data, and potential detriment to individuals.*	
Impact of the breach on Data Subject:	

Assess who should be notified: *List and state why – informing people and organisations that have experienced an incident can be an important element in helping to manage the situation. Notifying a person whose information got misdirected, for example, would help them to take precautions against ID theft, fraud etc. Also, consider if notification would serve only to worry them without any benefit; informing people about an incident is not an end in itself. Notification should have a clear purpose, whether this is to enable individuals who may have been affected to take steps to protect themselves or to allow the appropriate regulatory bodies to perform their functions, provide advice and deal with complaints.*	
Notification recommendation: *Tick all those that apply, adding additional information if required. Keep a record of the notification.*	
Evaluation: *Summarise the lessons learnt.* *Measures to be taken by the* Academy *to reduce the likelihood of such incidents from happening again:* *Consider adding to an action plan, with time for a review to check if measures have been implemented.*	
Senior staff sign off and recommendations:	The Head Teacher/Chair of Governors/DPO have read and reviewed the form and discussed the matters with relevant members of staff to reach the below conclusions: Agree/Do not agree [delete as applicable] with the assessment of risk and recommendations' The breach is not/is [delete as applicable] deemed reportable to the Information Commissioner. [Add additional points as required]
Signature:	
Name:	
Job title:	

Acknowledgements:

Andy Crow Chorus Business Advisers Ltd
Thomas Ng West Berkshire Council
Lizi Bird Solihull Metropolitan Borough Council

Amendments made by Tony Sheppard for the Academies Toolkit

Retention Guidelines

These retention guidelines are intended for use by Academy schools based in England and Wales. Academy schools based in Scotland should consult the Scottish Council on Archives retention documentation: http://www.scottisharchives.org.uk/scarrs/schedules.

1. The purpose of the retention guidelines

Under the Freedom of Information Act 2000, schools are required to maintain a retention schedule, listing the record series which the school creates in the course of its business. The retention schedule lays down the length of time over which the record needs to be retained, and the action which should be taken when it is of no further administrative use. The retention schedule lays down the basis for normal processing under the General Data Protection Regulation, Data Protection Act 2018 and the Freedom of Information Act 2000.

Members of staff are expected to manage their current recordkeeping systems using the retention schedule and to take account of differing retention periods when creating new recordkeeping systems.

The retention schedule refers to record series, regardless of the media in which they are stored.

2. Benefits of a retention schedule

There are numerous benefits which arise from the use of a complete retention schedule:

- Managing records against the retention schedule is deemed to be "normal processing" under the General Data Protection Regulation, Data Protection Act 2018 and the Freedom of Information Act 2000. Members of staff should be aware that once a Freedom of Information request is received or a legal hold imposed, then records disposal must be stopped.
- Members of staff can be confident that information has been disposed of safely and at the appropriate time.
- Information which is subject to the General Data Protection Regulation, Data Protection Act 2018 and the Freedom of Information Act 2000 legislation will be available when required.
- The school is not maintaining and storing information unnecessarily.

3. Maintaining and amending the retention schedule

Where appropriate, the retention schedule should be reviewed and amended to include any new record series created, as well as to remove any obsolete record series.

This retention schedule contains recommended retention periods for the various record series created and maintained by Academies in the course of their business. The schedule refers to all information, regardless of the media in which it is stored.

Some of the retention periods are governed by statute; others are guidelines following best practice. Every effort has been made to ensure that these retention periods are compliant with the requirements of the General Data Protection Regulation, Data Protection Act 2018 and the Freedom of Information Act 2000.

Managing record series using these retention guidelines will be deemed to be "normal processing" under the legislation mentioned above. If record series are to be kept for longer or shorter periods than those laid out in this document, the reasons for this need to be documented.

This schedule should be reviewed on a regular basis.

This document is a guideline only and liability falls on the end user and not on the IRMS. Individual organisations should seek appropriate legal advice as well as senior management approval. If required, Academies should consider purchasing a complete retention schedule. The IRMS can supply details of retention schedules which are available for sale.

The IRMS can only guarantee that these retention periods were correct at the time of going to press and that the retention schedule will be reviewed in a phased programme. Unless there is significant change in legislation, this retention schedule will be reviewed in 2021.

Questions will only be dealt with if they are submitted by IRMS members.

In order to submit a question, please complete the form on the webpage, remembering to include your IRMS membership number.

Further details about the benefits of IRMS membership can be found at: http://www.irms.org.uk/join

1. Governance, Funding and Financial Management of the Academy Trust

Academies are governed by the Academy Trust, which will usually be a company limited by guarantee[3]. The Academy Trust may also be a charitable trust.

1.1 Governance of the Academy Trust					
	Basic file description	**Data Protection Issues**	**Statutory Provisions**	**Retention Period [Operational]**	**Action at end of administrative life of the record**
1.1.1	Governance Statement	No		Life of governance statement + 6 years	SECURE DISPOSAL
1.1.2	Articles of Association	No		Life of the Academy	
1.1.3	Memorandum of Association	No		This can be disposed of once the Academy has been incorporated	SECURE DISPOSAL
1.1.4	Memorandum of Understanding of Shared Governance among Schools	No	*Companies Act 2006 section 355*	Life of Memorandum of Understanding + 6 years	SECURE DISPOSAL
1.1.5	Constitution	No		Life of the Academy	
1.1.6	Special Resolutions to amend the Constitution	No		Life of the Academy	
1.1.7	Written Scheme of Delegation	No	*Companies Act 2006 section 355*	Life of Written Scheme of Delegation + 10 years	SECURE DISPOSAL

[3] A **company limited by guarantee** does not usually have a share capital or shareholders, but instead has members who act as guarantors. The guarantors give an undertaking to contribute a nominal amount (typically very small) in the event of winding up of the **company**. In the case of an Academy, the guarantors will guarantee the sum of £10 each.

1.1 Governance of the Academy Trust					
	Basic file description	**Data Protection Issues**	**Statutory Provisions**	**Retention Period [Operational]**	**Action at end of administrative life of the record**
1.1.8	Directors – Appointment	No		Life of appointment + 6 years	SECURE DISPOSAL
1.1.9	Directors – Disqualification	No	Company Directors Disqualification Act 1986	Date of disqualification + 15 years	SECURE DISPOSAL
1.1.10	Directors – Termination of Office	No		Date of termination + 6 years	SECURE DISPOSAL
1.1.11	Annual Report – Trustees Report	No	*Companies Act 2006 section 355*	Date of report + 10 years	SECURE DISPOSAL
1.1.12	Annual Report and Accounts	No	*Companies Act 2006 section 355*	Date of report + 10 years	SECURE DISPOSAL
1.1.13	Annual Return	No	*Companies Act 2006 section 355*	Date of report + 10 years	SECURE DISPOSAL
1.1.14	Appointment of Trustees and Governors and Directors	Yes		Life of appointment + 6 years	SECURE DISPOSAL
1.1.15	Statement of Trustees Responsibilities	No		Life of appointment + 6 years	SECURE DISPOSAL
1.1.16	Appointment and removal of Members	No		Life of appointment + 6 years	SECURE DISPOSAL
1.1.17	Strategic Review	No		Date of the review + 6 years	SECURE DISPOSAL

1.1 Governance of the Academy Trust					
	Basic file description	**Data Protection Issues**	**Statutory Provisions**	**Retention Period [Operational]**	**Action at end of administrative life of the record**
1.1.18	Strategic Plan [also known as School Development Plans]	No		Life of plan + 6 years	SECURE DISPOSAL
1.1.19	Accessibility Plan	There may be if the plan refers to specific pupils	Limitation Act 1980 (Section 2)	Life of plan + 6 years	SECURE DISPOSAL

1.2	Board of Directors, Members Meetings and Governing Body				
	Basic file description	**Data Protection Issues**	**Statutory Provisions**	**Retention Period [Operational]**	**Action at end of administrative life of the record**
	Board of Directors				
1.2.1	Board Meeting Minutes	Could be if the minutes refer to living individuals	Companies Act 2006 section 248	Minutes must be kept for at least 10 years from the date of the meeting	OFFER TO ARCHIVES
1.2.2	Board Decisions	Could be if the decisions refer to living individuals		Date of the meeting + a minimum of 10 years	OFFER TO ARCHIVES
1.2.3	Board Meeting: Annual Schedule of Business	No		Current year	SECURE DISPOSAL
1.2.4	Board Meeting: Procedures for conduct of meeting	No	Limitation Act 1980 (Section 2)	Date procedures superseded + 6 years	SECURE DISPOSAL
	Committees[4]				
1.2.5	Minutes relating to any committees set up by the Board of Directors	Could be if the minutes refer to living individuals		Date of the meeting + a minimum of 10 years	OFFER TO ARCHIVES
	General Members' Meeting				

[4] The board can establish any committee and determine the constitution, membership and proceedings that will apply.

1.2	Board of Directors, Members Meetings and Governing Body				
	Basic file description	**Data Protection Issues**	**Statutory Provisions**	**Retention Period [Operational]**	**Action at end of administrative life of the record**
1.2.6	Records relating to the management of General Members' Meetings	Could be if the minutes refer to living individuals	Companies Act 2006 section 248	Minutes must be kept for at least 10 years from the date of the meeting[5]	OFFER TO ARCHIVES
1.2.7	Records relating to the management of the Annual General Meeting[6]	Could be if the minutes refer to living individuals	Companies Act 2006 section 248	Minutes must be kept for at least 10 years from the date of the meeting[7]	OFFER TO ARCHIVES
	Governors				
1.2.8	**Agendas for Governing Body meetings**	May be data protection issues, if the meeting is dealing with confidential issues relating to staff		One copy should be retained with the master set of minutes. All other copies can be disposed of	SECURE DISPOSAL[8]

[5] The signed minutes must be kept securely together with the notice and agenda for the meeting and supporting documentation provided for consideration at the meeting. Documentation is generally filed in a dedicated minute book, which is usually in the form of a loose-leaf binder to which additional pages can be easily added.

[6] Not all Academies are required to hold an Annual General Meeting for the Members – the requirement will be stated in the Constitution.

[7] The signed minutes must be kept securely together with the notice and agenda for the meeting and any supporting documentation provided for consideration at the meeting. Documentation is generally filed in a dedicated minute book, which is usually in the form of a loose-leaf binder to which additional pages can be easily added.

[8] In this context, SECURE DISPOSAL should be taken to mean disposal using confidential waste bins, or if the school has the facility, shredding using a cross-cut shredder.

1.2	Board of Directors, Members Meetings and Governing Body				
	Basic file description	**Data Protection Issues**	**Statutory Provisions**	**Retention Period [Operational]**	**Action at end of administrative life of the record**
1.2.9	Minutes of, and papers considered at, meetings of the Governing Body and its committees	May be data protection issues, if the meeting is dealing with confidential issues relating to staff			
	Principal Set (signed)			Life of Academy	
	Inspection Copies[9]			Date of meeting + 3 years	SECURE DISPOSAL
1.2.10	Reports presented to the Governing Body	May be data protection issues, if the report deals with confidential issues relating to staff		Reports should be kept for a minimum of 6 years. However, if the minutes refer directly to individual reports, then the reports should be kept for the life of the Academy	SECURE DISPOSAL or retain with the signed set of minutes

[9] These are the copies which the clerk to the Governor may wish to retain, so that requestors can view all the relevant information, without the clerk needing to print off and collate redacted copies of the minutes each time a request is made.

1.2	Board of Directors, Members Meetings and Governing Body				
	Basic file description	**Data Protection Issues**	**Statutory Provisions**	**Retention Period [Operational]**	**Action at end of administrative life of the record**
1.2.11	Meeting papers relating to the annual parents' meeting held under Section 33 of the Education Act 2002	No	Education Act 2002, Section 33	Date of the meeting + a minimum of 6 years	SECURE DISPOSAL
1.2.12	Trusts and Endowments managed by the Governing Body	No		PERMANENT	
1.2.13	Records relating to complaints dealt with by the Governing Body	Yes		Date of the resolution of the complaint + a minimum of 6 years then review for further retention in case of contentious disputes	SECURE DISPOSAL
1.2.14	Annual Reports created under the requirements of the Education (Governor's Annual Reports) (England) (Amendment) Regulations 2002	No	Education (Governor's Annual Reports) (England) (Amendment) Regulations 2002 SI 2002 No 1171	Date of report + 10 years	SECURE DISPOSAL

1.2	Board of Directors, Members Meetings and Governing Body				
	Basic file description	**Data Protection Issues**	**Statutory Provisions**	**Retention Period [Operational]**	**Action at end of administrative life of the record**
	Statutory Registers[10]				
1.2.15	Register of Directors		Companies Act 2006	Life of the Academy + 6 years	SECURE DISPOSAL
1.2.16	Register of Directors' interests [this is not a statutory register]			Life of the Academy + 6 years	SECURE DISPOSAL
1.2.17	Register of Directors' residential addresses		Companies Act 2006	Life of the Academy + 6 years	SECURE DISPOSAL
1.2.18	Register of gifts, hospitality and entertainments		Companies Act 2006	Life of the Academy + 6 years	SECURE DISPOSAL
1.2.19	Register of members		Companies Act 2006	Life of the Academy + 6 years	SECURE DISPOSAL
1.2.20	Register of secretaries		Companies Act 2006	Life of the Academy + 6 years	SECURE DISPOSAL
1.2.21	Register of Trustees interests			Life of the Academy + 6 years	SECURE DISPOSAL
1.2.22	Declaration of Interests Statements [Governors] [this is not a statutory register]			Life of the Academy + 6 years	SECURE DISPOSAL

[10] Academies are required by law to keep specific records, collectively known as statutory registers or the statutory books. The registers record information relating to the Academy's operations and structure, such as the current directors. Records should be kept up-to-date to reflect any changes that take place.

1.3	Funding and Finance				
	Basic file description	**Data Protection Issues**	**Statutory Provisions**	**Retention Period [Operational]**	**Action at end of administrative life of the record**
	Strategic Finance				
1.3.1	Statement of financial activities for the year	No		Current financial year + 6 years	SECURE DISPOSAL
1.3.2	Financial planning	No		Current financial year + 6 years	SECURE DISPOSAL
1.3.3	Value for money statement	No		Current financial year + 6 years	SECURE DISPOSAL
1.3.4	Records relating to the management of VAT	No		Current financial year + 6 years	SECURE DISPOSAL
1.3.5	Whole of government accounts returns	No		Current financial year + 6 years	SECURE DISPOSAL
1.3.6	Borrowing powers	No		Current financial year + 6 years	SECURE DISPOSAL
1.3.7	Budget plan	No		Current financial year + 6 years	SECURE DISPOSAL
1.3.8	Charging and remissions policy	No		Date policy superseded + 3 years	SECURE DISPOSAL
	Audit Arrangements				
1.3.9	Audit Committee and appointment of responsible officers	No		Life of the Academy	SECURE DISPOSAL
1.3.10	Independent Auditor's report on regularity	No		Financial year report relates to + 6 years	SECURE DISPOSAL
1.3.11	Independent Auditor's report on financial statements	No		Financial year report relates to + 6 years	SECURE DISPOSAL

1.3	Funding and Finance				
	Basic file description	**Data Protection Issues**	**Statutory Provisions**	**Retention Period [Operational]**	**Action at end of administrative life of the record**
	Funding Agreements				
1.3.12	Funding Agreement with Secretary of State and supplemental funding agreements11	No		Date of last payment of funding + 6 years	SECURE DISPOSAL
1.3.13	Funding Agreement – Termination of the funding agreement12			Date of last payment of funding + 6 years	SECURE DISPOSAL
1.3.14	Funding Records – Capital Grant	No		Date of last payment of funding + 6 years	SECURE DISPOSAL
1.3.15	Funding Records – Earmarked Annual Grant (EAG)	No		Date of last payment of funding + 6 years	SECURE DISPOSAL
1.3.16	Funding Records – General Annual Grant (GAG)	No		Date of last payment of funding + 6 years	SECURE DISPOSAL
1.3.17	Per pupil funding records	No		Date of last payment of funding + 6 years	SECURE DISPOSAL
1.3.18	Exclusions agreement13	No		Date of last payment of funding + 6 years	SECURE DISPOSAL

11 Where there is multi-Academy governance.
12 Either party may give not less than 7 financial years' written notice to terminate the Agreement, such notice to expire on 31 August. Or, where the Academy has significant financial issues or is insolvent, the Agreement can be terminated by the Secretary of State to take effect on the date of the notice.
13 The Academy can enter into an arrangement with a Local Authority (LA), so that payment will flow between the Academy and the LA, in the same way as it would do were the Academy a maintained school.

1.3 Funding and Finance					
	Basic file description	**Data Protection Issues**	**Statutory Provisions**	**Retention Period [Operational]**	**Action at end of administrative life of the record**
1.3.19	Funding records[14]	No		Date of last payment of funding + 6 years	SECURE DISPOSAL
1.3.20	Gift Aid and Tax Relief	No		Date of last payment of funding + 6 years	SECURE DISPOSAL
1.3.21	Records relating to loans	No		Date of last payment on loan + 6 years if the loan is under £10,000 or date of last payment on loan + 12 years if the loan is over £10,000	SECURE DISPOSAL
	Payroll and Pensions				
1.3.22	Maternity pay records	Yes	Statutory Maternity Pay (General) Regulations 1986 (SI1986/1960), revised 1999 (SI1999/567)	Current year + 3 years	SECURE DISPOSAL

[14] Funding agreement which says that the Academy can receive donations and can only charge where the law allows maintained schools to charge [see Charging and Remission Policy].

1.3 Funding and Finance					
	Basic file description	**Data Protection Issues**	**Statutory Provisions**	**Retention Period [Operational]**	**Action at end of administrative life of the record**
1.3.23	Records held under Retirement Benefits Schemes (Information Powers) Regulations 1995	Yes	Regulation 15 Retirement Benefits Schemes (Information Powers) Regulations 1995 (SI 1995/3103)	From the end of the year in which the accounts were signed for a minimum of 6 years	SECURE DISPOSAL
1.3.24	Management of the Teachers' Pension Scheme	Yes		Date of last payment on the pension + 6 years	SECURE DISPOSAL
1.3.25	Records relating to pension registrations	Yes		Date of last payment on the pension + 6 years	SECURE DISPOSAL
1.3.26	Payroll records	Yes		Date payroll run + 6 years	SECURE DISPOSAL
	Risk Management and Insurance				
1.3.27	Insurance policies	No		Date the policy expires + 6 years	SECURE DISPOSAL
1.3.28	Records relating to the settlement of insurance claims	No		Date claim settled + 6 years	SECURE DISPOSAL
1.3.29	Employer's Liability Insurance Certificate	No		Closure of the school + 40 years	SECURE DISPOSAL
	Endowment Funds and Investments				
1.3.30	Investment policies	No		Life of the investment + 6 years	SECURE DISPOSAL

1.3 Funding and Finance					
	Basic file description	**Data Protection Issues**	**Statutory Provisions**	**Retention Period [Operational]**	**Action at end of administrative life of the record**
1.3.31	Management of Endowment Funds	No		Life of the fund + 6 years	
	Accounts and Statements				
1.3.32	Annual accounts	No		Current year + 6 years	STANDARD DISPOSAL
1.3.33	Loans and grants managed by the school	No		Date of last payment on the loan + 12 years then REVIEW	SECURE DISPOSAL
1.3.34	Student Grant applications	Yes		Current year + 3 years	SECURE DISPOSAL
1.3.35	All records relating to the creation and management of budgets, including the Annual Budget statement and background papers	No		Life of the budget + 3 years	SECURE DISPOSAL
1.3.36	Invoices, receipts, order books and requisitions, delivery notices	No		Current financial year + 6 years	SECURE DISPOSAL
1.3.37	Records relating to the collection and banking of monies	No		Current financial year + 6 years	SECURE DISPOSAL

1.3 Funding and Finance					
	Basic file description	**Data Protection Issues**	**Statutory Provisions**	**Retention Period [Operational]**	**Action at end of administrative life of the record**
1.3.38	Records relating to the identification and collection of debt	No		Current financial year + 6 years	SECURE DISPOSAL
	Contract Management				
1.3.39	All records relating to the management of contracts under seal	No	Limitation Act 1980	Last payment on the contract + 12 years	SECURE DISPOSAL
1.3.40	All records relating to the management of contracts under signature	No	Limitation Act 1980	Last payment on the contract + 6 years	SECURE DISPOSAL
1.3.41	Records relating to the monitoring of contracts	No		Current year + 2 years	SECURE DISPOSAL
	Asset Management				
1.3.42	Inventories of furniture and equipment	No		Current year + 6 years	SECURE DISPOSAL
1.3.43	Burglary, theft and vandalism report forms	No		Current year + 6 years	SECURE DISPOSAL
1.3.44	Records relating to the leasing of shared facilities, such as sports centres	No		Current year + 6 years	SECURE DISPOSAL
1.3.45	Land and building valuations	No		Date valuation superseded + 6 years	SECURE DISPOSAL

1.3 Funding and Finance					
	Basic file description	**Data Protection Issues**	**Statutory Provisions**	**Retention Period [Operational]**	**Action at end of administrative life of the record**
1.3.46	Disposal of assets	No		Date asset disposed of + 6 years	SECURE DISPOSAL
1.3.47	Community School leases for land	No		Date lease expires + 6 years	SECURE DISPOSAL
1.3.48	Commercial transfer arrangements	No		Date of transfer + 6 years	SECURE DISPOSAL
1.3.49	Transfer of land to the Academy Trust	No		Life of land ownership then transfer to new owner	SECURE DISPOSAL
1.3.50	Transfers of freehold land	No		Life of land ownership then transfer to new owner	SECURE DISPOSAL
	School Fund				
1.3.51	School Fund – Cheque books	No		Current year + 6 years	SECURE DISPOSAL
1.3.52	School Fund – Paying in books	No		Current year + 6 years	SECURE DISPOSAL
1.3.53	School Fund – Ledger	No		Current year + 6 years	SECURE DISPOSAL
1.3.54	School Fund – Invoices	No		Current year + 6 years	SECURE DISPOSAL
1.3.55	School Fund – Receipts	No		Current year + 6 years	SECURE DISPOSAL
1.3.56	School Fund – Bank statements	No		Current year + 6 years	SECURE DISPOSAL

1.3	Funding and Finance				
	Basic file description	**Data Protection Issues**	**Statutory Provisions**	**Retention Period [Operational]**	**Action at end of administrative life of the record**
1.3.57	School Fund – Journey books	No		Current year + 6 years	SECURE DISPOSAL
	School Meals[15]				
1.3.58	Free school meals registers	Yes		Current year + 6 years	SECURE DISPOSAL
1.3.59	School meals registers	Yes		Current year + 3 years	SECURE DISPOSAL
1.3.60	School meals summary sheets	No		Current year + 3 years	SECURE DISPOSAL

As a charity, an Academy is not permitted to trade and make a profit. It is, however, possible to set up a subsidiary trading company, which can sell products or services and Gift Aid profits back to the Academy. If the Academy operates a subsidiary company, it is expected that these records will be managed in line with standard business practice.

1.4	Policies, Frameworks and Overarching Requirements				
	Basic file description	**Data Protection Issues**	**Statutory Provisions**	**Retention Period [Operational]**	**Action at end of administrative life of the record**
1.4.1	Data Protection Policy, including data protection notification	No		Date policy superseded + 6 years	SECURE DISPOSAL
1.4.2	Freedom of Information Policy	No		Date policy superseded + 6 years	SECURE DISPOSAL

15 Unless it would be unreasonable to do so, school lunches should be provided when they are requested by, or on behalf of, any pupil. A school lunch must be provided free of charge to any pupil entitled to free school lunches. From September 2014, free school lunches must be provided to all KS1 pupils.

1.4	Policies, Frameworks and Overarching Requirements				
	Basic file description	**Data Protection Issues**	**Statutory Provisions**	**Retention Period [Operational]**	**Action at end of administrative life of the record**
1.4.3	Information Security Breach Policy	No		Date policy superseded + 6 years	SECURE DISPOSAL
1.4.4	Special Educational Needs Policy	No		Date policy superseded + 6 years	SECURE DISPOSAL
1.4.5	Complaints Policy	No		Date policy superseded + 6 years	SECURE DISPOSAL
1.4.6	Risk and Control Framework	No		Life of framework + 6 years	SECURE DISPOSAL
1.4.7	Rules and Bylaws	No		Date rules or bylaws superseded + 6 years	SECURE DISPOSAL
1.4.9	Home School Agreements[16]	No		Date agreement revised + 6 years	SECURE DISPOSAL
1.4.10	Equality Information and Objectives (public sector equality duty) Statement for publication	No		Date of statement + 6 years	SECURE DISPOSAL

[16] This should be drawn up in consultation with parents and should apply to all pupils.

2. Human Resources

2.1 Recruitment[17]					
	Basic file description	**Data Protection Issues**	**Statutory Provisions**	**Retention Period [Operational]**	**Action at end of administrative life of the record**
2.1.1	All records leading up to the appointment of a new Head Teacher	Yes		Date of appointment + 6 years	SECURE DISPOSAL
2.1.2	All records leading up to the appointment of a new member of staff – unsuccessful candidates	Yes		Date of appointment of successful candidate + 6 months	SECURE DISPOSAL
2.1.3	All records leading up to the appointment of a new member of staff – successful candidate	Yes		All relevant information should be added to the Staff Personal File (see below) and all other information retained for 6 months	SECURE DISPOSAL
2.1.4	Pre-employment vetting information – DBS Checks[18]	No	DBS Update Service Employer Guide June 2014	The organisation should take a copy of the DBS certificate when it is shown to them by the individual and should be added to the Staff Personal File	SECURE DISPOSAL
2.1.5	Proofs of identity collected as part of the process of checking "portable" enhanced DBS disclosure	Yes		Where possible, these should be checked, and a note kept of what was seen and what has been checked. If it is felt necessary to keep copy documentation, then this should be added to the Staff Personal File	SECURE DISPOSAL

[17] Academies do not necessarily have to employ people with qualified teacher status; only the SEN and designated LAC teacher must be qualified.
[18] Academies are bound by the legislation that applies to independent schools NOT maintained schools.

2.1 Recruitment[17]					
	Basic file description	**Data Protection Issues**	**Statutory Provisions**	**Retention Period [Operational]**	**Action at end of administrative life of the record**
2.1.6	Pre-employment vetting information – Evidence proving the right to work in the United Kingdom[19]	Yes	An employer's guide to right to work checks [Home Office May 2015]	Where possible, these documents should be added to the Staff Personal File, but if they are kept separately, then the Home Office requires that the documents are kept for termination of employment plus not less than 2 years	SECURE DISPOSAL
2.1.7	Records relating to the employment of overseas teachers	Yes		Where possible, these documents should be added to the Staff Personal File, but if they are kept separately, then the Home Office requires that the documents are kept for termination of employment plus not less than 2 years	SECURE DISPOSAL
2.1.8	Records relating to the TUPE process	Yes		Date last member of staff transfers or leaves the organisation + 6 years	SECURE DISPOSAL

[19] Employers are required to take a "clear copy" of the documents which they are shown as part of this process.

2.2 Operational Staff Management					
	Basic file description	**Data Protection Issues**	**Statutory Provisions**	**Retention Period [Operational]**	**Action at end of administrative life of the record**
2.2.1	Staff Personal File, including employment contract and staff training records	Yes	Limitation Act 1980 (Section 2)	Termination of employment + 6 years	SECURE DISPOSAL
2.2.2	Timesheets	Yes		Current year + 6 years	SECURE DISPOSAL
2.2.3	Annual appraisal/assessment records	Yes		Current year + 5 years	SECURE DISPOSAL
2.2.4	Records relating to the agreement of pay and conditions	No		Date pay and conditions superseded + 6 years	SECURE DISPOSAL
2.2.5	Training needs analysis	No		Current year + 1 year	SECURE DISPOSAL

2.3 Management of Disciplinary and Grievance Processes					
	Basic file description	**Data Protection Issues**			
2.3.1	Allegation which is child protection in nature against a member of staff, including where the allegation is unfounded[20]	Yes	"Keeping children safe in education Statutory guidance for schools and colleges March 2015"; "Working together to safeguard children. A guide to inter-agency working to safeguard and promote the welfare of children March 2015"	Until the person's normal retirement age or 10 years from the date of the allegation, whichever is longer, then REVIEW	SECURE DISPOSAL These records must be shredded
2.3.2	Disciplinary Proceedings	Yes			
	• Oral warning			Date of warning[21] + 6 months	SECURE DISPOSAL[22]
	• Written warning – level 1			Date of warning + 6 months	SECURE DISPOSAL[23]
	• Written warning – level 2			Date of warning + 12 months	SECURE DISPOSAL[24]
	• Final warning			Date of warning + 18 months	SECURE DISPOSAL[25]

[20] This review took place when the Independent Inquiry on Child Sexual Abuse was beginning. In light of this, it is recommended that all records relating to child abuse are retained until the Inquiry is completed. This section will then be reviewed again to take into account any recommendations the Inquiry might make concerning record retention.

[21] Where the warning relates to child protection issues, see above. If the disciplinary proceedings relate to a child protection matter, please contact your Safeguarding Children Officer for further advice.

[22] If warnings are placed on personal files, then they must be weeded from the file.

[23] If warnings are placed on personal files, then they must be weeded from the file.

[24] If warnings are placed on personal files, then they must be weeded from the file.

[25] If warnings are placed on personal files, then they must be weeded from the file.

2.3 Management of Disciplinary and Grievance Processes					
	Basic file description	**Data Protection Issues**			
	• Case not found			If the incident is child protection related, then see above; otherwise, dispose of at the conclusion of the case	SECURE DISPOSAL

2.4 Health and Safety					
	Basic file description	**Data Protection Issues**	**Statutory Provisions**	**Retention Period [Operational]**	**Action at end of administrative life of the record**
2.4.1	Health and Safety policy statements	No		Life of policy + 3 years	SECURE DISPOSAL
2.4.2	Health and Safety risk assessments	No		Life of risk assessment + 3 years	SECURE DISPOSAL
2.4.3	Records relating to accident/injury at work	Yes		Date of incident + 12 years In the case of serious accidents, a further retention period will need to be applied	SECURE DISPOSAL

2.4 Health and Safety					
	Basic file description	**Data Protection Issues**	**Statutory Provisions**	**Retention Period [Operational]**	**Action at end of administrative life of the record**
2.4.4	Accident reporting	Yes	Social Security (Claims and Payments) Regulations 1979 Regulation 25. Social Security Administration Act 1992 Section 8. Limitation Act 1980	The official Accident Book must be retained for 3 years after the last entry in the book. The book may be in paper or electronic format The incident reporting form may be retained as below	
	• Adults			Date of incident + 6 years	SECURE DISPOSAL
	• Children			Date of birth of the child + 25 years	SECURE DISPOSAL
2.4.5	Control of Substances Hazardous to Health (COSHH)	No		Current year + 10 years then REVIEW	SECURE DISPOSAL
2.4.6	Process of monitoring of areas where employees and persons are likely to have come into contact with asbestos	No		Last action + 40 years	SECURE DISPOSAL
2.4.7	Process of monitoring of areas where employees and persons are likely to have come into contact with radiation	No		Last action + 50 years	SECURE DISPOSAL
2.4.8	Fire precautions log books	No		Current year + 6 years	SECURE DISPOSAL
2.4.9	Fire risk assessments	No	Fire Service Order 2005	Life of the risk assessment + 6 years	SECURE DISPOSAL

2.4 Health and Safety					
	Basic file description	**Data Protection Issues**	**Statutory Provisions**	**Retention Period [Operational]**	**Action at end of administrative life of the record**
2.4.10	Incident reports	Yes		Current year + 20 years	SECURE DISPOSAL

3. Management of the Academy

3.1 Admissions					
	Basic file description	**Data Protection Issues**	**Statutory Provisions**	**Retention Period [Operational]**	**Action at end of administrative life of the record**
3.1.1	All records relating to the creation and implementation of the School Admissions' Policy	No	School Admissions Code Statutory Guidance for admission authorities, governing bodies, local authorities, schools' adjudicators and admission appeals panels December 2014	Life of the policy + 3 years then REVIEW	SECURE DISPOSAL
3.1.2	Admissions – if the admission is successful	Yes	School Admissions Code Statutory Guidance for admission authorities, governing bodies, local authorities, schools' adjudicators and admission appeals panels December 2014	Date of admission + 1 year	SECURE DISPOSAL

3.1 Admissions					
	Basic file description	**Data Protection Issues**	**Statutory Provisions**	**Retention Period [Operational]**	**Action at end of administrative life of the record**
3.1.3	Admissions – if the appeal is unsuccessful	Yes	School Admissions Code Statutory Guidance for admission authorities, governing bodies, local authorities, schools' adjudicators and admission appeals panels December 2014	Resolution of case + 1 year	SECURE DISPOSAL
3.1.4	Register of admissions	Yes	School attendance: Departmental advice for maintained schools, Academies, independent schools and local authorities October 2014	Every entry in the admission register must be preserved for a period of 3 years after the date on which the entry was made[26]	REVIEW Schools may wish to consider keeping the admission register permanently, as often schools receive enquiries from past pupils to confirm the dates they attended the school
3.1.5	Admissions – Secondary Schools – Casual	Yes		Current year + 1 year	SECURE DISPOSAL

[26] School attendance: Departmental advice for maintained schools, Academies, independent schools and local authorities October 2014 p6.

3.1 Admissions					
	Basic file description	**Data Protection Issues**	**Statutory Provisions**	**Retention Period [Operational]**	**Action at end of administrative life of the record**
3.1.6	Proofs of address supplied by parents as part of the admissions process	Yes	School Admissions Code Statutory Guidance for admission authorities, governing bodies, local authorities, schools' adjudicators and admission appeals panels December 2014	Current year + 1 year	SECURE DISPOSAL
3.1.7	Supplementary information form, including additional information such as religion and medical conditions	Yes			
	• For successful admissions			This information should be added to the pupil file	SECURE DISPOSAL
	• For unsuccessful admissions			Until appeals process completed	SECURE DISPOSAL

3.2 Head Teacher and Senior Management Team					
	Basic file description	**Data Protection Issues**	**Statutory Provisions**	**Retention Period [Operational]**	**Action at end of administrative life of the record**
3.2.1	Log books of activity in the school maintained by the Head Teacher	There may be data protection issues if the log book refers to individual pupils or members of staff		Date of last entry in the book + a minimum of 6 years then REVIEW	These could be of permanent historical value and should be offered to the County Archives Service, if appropriate
3.2.2	Minutes of Senior Management Team meetings and meetings of other internal administrative bodies	There may be data protection issues if the minutes refers to individual pupils or members of staff		Date of the meeting + 3 years then REVIEW	SECURE DISPOSAL
3.2.3	Reports created by the Head Teacher or the Management Team	There may be data protection issues if the report refers to individual pupils or members of staff		Date of the report + a minimum of 3 years then REVIEW	SECURE DISPOSAL
3.2.4	Records created by Head Teachers, Deputy Head Teachers, heads of year and other members of staff with administrative responsibilities	There may be data protection issues if the records refer to individual pupils or members of staff		Current academic year + 6 years then REVIEW	SECURE DISPOSAL
3.2.5	Correspondence created by Head Teachers, Deputy Head Teachers, heads of year and other members of staff with administrative responsibilities	There may be data protection issues if the correspondence refers to individual pupils or members of staff		Date of correspondence + 3 years then REVIEW	SECURE DISPOSAL
3.2.6	Professional Development Plans	Yes		Life of the plan + 6 years	SECURE DISPOSAL

3.3 Operational Administration					
	Basic file description	**Data Protection Issues**	**Statutory Provisions**	**Retention Period [Operational]**	**Action at end of administrative life of the record**
3.3.1	Management of complaints	Yes		Date complaint resolved + 3 years	SECURE DISPOSAL
3.3.2	Records relating to the management of contracts with external providers	No		Date of last payment on contract + 6 years	SECURE DISPOSAL
3.3.3	Records relating to the management of software licences	No		Date licence expires + 6 years	SECURE DISPOSAL
3.3.4	General file series	No		Current year + 5 years then REVIEW	SECURE DISPOSAL
3.3.5	Records relating to the creation and publication of the school brochure or prospectus	No		Current year + 3 years	STANDARD DISPOSAL
3.3.6	Records relating to the creation and distribution of circulars to staff, parents or pupils	No		Current year + 1 year	STANDARD DISPOSAL
3.3.7	Newsletters and other items with a short operational use	No		Current year + 1 year	STANDARD DISPOSAL
3.3.8	Visitors' books and signing in sheets	Yes		Current year + 6 years then REVIEW	SECURE DISPOSAL
3.3.9	Records relating to the creation and management of Parent Teacher Associations and/or Old Pupils Associations	No		Current year + 6 years then REVIEW	SECURE DISPOSAL

4. Property Management

This section covers the management of buildings and property.

4.1 Property Management					
	Basic file description	**Data Protection Issues**	**Statutory Provisions**	**Retention Period [Operational]**	**Action at end of administrative life of the record**
4.1.1	Title deeds of properties belonging to the school	No		These should follow the property, unless the property has been registered with the Land Registry	
4.1.2	Plans of property belonging to the school	No		These should be retained whilst the building belongs to the school and should be passed onto any new owners if the building is leased or sold	
4.1.3	Leases of property leased by or to the school	No		Expiry of lease + 6 years	SECURE DISPOSAL
4.1.4	Records relating to the letting of school premises	No		Current financial year + 6 years	SECURE DISPOSAL
4.1.5	Business continuity and disaster recovery plans	No		Date the plan superseded + 3 years	SECURE DISPOSAL

4.2 Maintenance					
	Basic file description	**Data Protection Issues**	**Statutory Provisions**	**Retention Period [Operational]**	**Action at end of administrative life of the record**
4.2.1	All records relating to the maintenance of the school carried out by contractors	No		Current year + 6 years	SECURE DISPOSAL
4.2.2	All records relating to the maintenance of the school carried out by school employees, including maintenance log books	No		Current year + 6 years	SECURE DISPOSAL

4.3 Fleet Management					
	Basic file description	**Data Protection Issues**	**Statutory Provisions**	**Retention Period [Operational]**	**Action at end of administrative life of the record**
4.3.1	The process of acquisition and disposal of vehicles through lease or purchase, e.g., contracts/leases, quotes, approvals	N	Limitation Act 1980 (Section 2)	Disposal of the vehicle + 6 years	SECURE DISPOSAL
4.3.2	The process of managing allocation and maintenance of vehicles, e.g., lists of who was driving the vehicles and when, maintenance	N	Limitation Act 1980 (Section 2)	Disposal of the vehicle + 6 years	SECURE DISPOSAL
4.3.3	Service logs and vehicle logs	N	Limitation Act 1980 (Section 2)	Life of the vehicle, then either to be retained for 6 years by school or to be returned to lease company	SECURE DISPOSAL
4.3.4	GPS tracking data relating to the vehicles	N	Limitation Act 1980 (Section 2)	Date of journey + 6 years	SECURE DISPOSAL

5. Pupil Management

This section includes all records which are created during the time a pupil spends at the school. For information about accident reporting, see under Health and Safety above.

5.1 Pupil's Educational Record					
	Basic file description	**Data Protection Issues**	**Statutory Provisions**	**Retention Period [Operational]**	**Action at end of administrative life of the record**
5.1.1	Pupil's Educational Record required by The Education (Pupil Information) (England) Regulations 2005	Yes	The Education (Pupil Information) (England) Regulations 2005 SI 2005 No. 1437		
	• Primary			Retain whilst the child remains at the primary school	The file should follow the pupil when they leave the primary school. This will include: • To another primary school • To a secondary school • To a pupil referral unit If the pupil dies whilst at primary school, the file should be returned to the LA to be retained for the statutory retention period. If the pupil transfers to an independent school, transfers to home schooling or leaves the country, the file should be returned to the LA to be retained for the statutory retention period. Primary schools do not ordinarily

5.1 Pupil's Educational Record					
	Basic file description	**Data Protection Issues**	**Statutory Provisions**	**Retention Period [Operational]**	**Action at end of administrative life of the record**
					have sufficient storage space to store records for pupils who have not transferred in the normal way. It makes more sense to transfer the record to the LA, as it is more likely that the pupil will request the record from the LA
	• Secondary		Limitation Act 1980 (Section 2)	Date of birth of the pupil + 25 years	SECURE DISPOSAL
5.1.2	Records relating to the management of exclusions	Yes		Date of birth of the pupil involved + 25 years	SECURE DISPOSAL
5.1.3	Management of examination registrations	Yes		The examination board will usually mandate how long these records need to be retained	
5.1.4	Examination results – pupil copies	Yes			
	• Public			This information should be added to the pupil file	All uncollected certificates should be returned to the examination board
	• Internal			This information should be added to the pupil file	
	This review took place when the Independent Inquiry on Historical Child Sexual Abuse was beginning. In light of this, it is recommended that all records relating to child abuse are retained until the Inquiry is completed. This section will then be reviewed again to take into account any recommendations the Inquiry might make concerning record retention				

5.1 Pupil's Educational Record					
	Basic file description	**Data Protection Issues**	**Statutory Provisions**	**Retention Period [Operational]**	**Action at end of administrative life of the record**
5.1.5	Child protection information held on pupil file	Yes	"Keeping children safe in education Statutory guidance for schools and colleges March 2015"; "Working together to safeguard children. A guide to inter-agency working to safeguard and promote the welfare of children March 2015"	If any records relating to child protection issues are placed on the pupil file, it should be in a sealed envelope and then retained for the same period of time as the pupil file	SECURE DISPOSAL – these records MUST be shredded
5.1.6	Child protection information held in separate files	Yes	"Keeping children safe in education Statutory guidance for schools and colleges March 2015"; "Working together to safeguard children. A guide to inter-agency working to safeguard and promote the welfare of children March 2015"	Date of birth of the child + 25 years then REVIEW This retention period was agreed in consultation with the Safeguarding Children Group on the understanding that the principal copy of this information will be found on the LA Social Services record	SECURE DISPOSAL – these records MUST be shredded

Retention periods relating to allegations made against adults can be found in the Human Resources section of this retention schedule.

5.2 Attendance					
	Basic file description	**Data Protection Issues**	**Statutory Provisions**	**Retention Period [Operational]**	**Action at end of administrative life of the record**
5.2.1	Attendance registers	Yes	School attendance: Departmental advice for maintained schools, Academies, independent schools and local authorities October 2014	Every entry in the attendance register must be preserved for a period of 3 years after the date on which the entry was made	SECURE DISPOSAL
5.2.2	Correspondence relating to authorised absence		Education Act 1996 Section 7	Current academic year + 2 years	SECURE DISPOSAL

5.3 Special Educational Needs					
	Basic file description	**Data Protection Issues**	**Statutory Provisions**	**Retention Period [Operational]**	**Action at end of administrative life of the record**
5.3.1	Special Educational Needs files, reviews and Individual Education Plans	Yes	Limitation Act 1980 (Section 2)	Date of birth of the pupil + 25 years	REVIEW NOTE: This retention period is the minimum retention period that any pupil file should be kept. Some authorities choose to keep SEN files for a longer period of time in order to defend themselves in a “failure to provide a sufficient education” case. There is an element of business risk analysis involved in any decision to keep the records longer than the minimum retention period – this should be documented

5.3 Special Educational Needs					
	Basic file description	**Data Protection Issues**	**Statutory Provisions**	**Retention Period [Operational]**	**Action at end of administrative life of the record**
5.3.2	Statement maintained under section 234 of the Education Act 1990 and any amendments made to the statement	Yes	Education Act 1996 Special Educational Needs and Disability Act 2001 Section 1	Date of birth of the pupil + 25 years [This would normally be retained on the pupil file]	SECURE DISPOSAL, unless the document is subject to a legal hold
5.3.3	Advice and information provided to parents regarding educational needs	Yes	Special Educational Needs and Disability Act 2001 Section 2	Date of birth of the pupil + 25 years [This would normally be retained on the pupil file]	SECURE DISPOSAL, unless the document is subject to a legal hold
5.3.4	Accessibility strategy	Yes	Special Educational Needs and Disability Act 2001 Section 14	Date of birth of the pupil + 25 years [This would normally be retained on the pupil file]	SECURE DISPOSAL, unless the document is subject to a legal hold

6. Curriculum Management

6.1 Statistics and Management Information					
	Basic file description	**Data Protection Issues**	**Statutory Provisions**	**Retention Period [Operational]**	**Action at end of administrative life of the record**
6.1.1	Curriculum returns	No		Current year + 3 years	SECURE DISPOSAL
6.1.2	Examination results (schools copy)	Yes		Current year + 6 years	SECURE DISPOSAL
	SATs records –	Yes			
	• Results			The SATS results should be recorded on the pupil's educational file and will therefore be retained until the pupil reaches the age of 25 years The school may wish to keep a composite record of all the whole year SATs results. These could be kept for current year + 6 years to allow suitable comparison	SECURE DISPOSAL
	• Examination papers			The examination papers should be kept until any appeals/validation process is complete	SECURE DISPOSAL
6.1.3	Published Admission Number (PAN) reports	Yes		Current year + 6 years	SECURE DISPOSAL
6.1.4	Value added and contextual data	Yes		Current year + 6 years	SECURE DISPOSAL
6.1.5	Self-evaluation forms	Yes		Current year + 6 years	SECURE DISPOSAL

6.2 Implementation of Curriculum					
	Basic file description	**Data Protection Issues**	**Statutory Provisions**	**Retention Period [Operational]**	**Action at end of administrative life of the record**
6.2.1	Schemes of work	No		Current year + 1 year	It may be appropriate to review these records at the end of each year and allocate a further retention period, or, SECURE DISPOSAL
6.2.2	Timetable	No		Current year + 1 year	It may be appropriate to review these records at the end of each year and allocate a further retention period, or, SECURE DISPOSAL
6.2.3	Class record books	No		Current year + 1 year	It may be appropriate to review these records at the end of each year and allocate a further retention period, or, SECURE DISPOSAL
6.2.4	Mark books	No		Current year + 1 year	It may be appropriate to review these records at the end of each year and allocate a further retention period, or, SECURE DISPOSAL
6.2.5	Record of homework set	No		Current year + 1 year	It may be appropriate to review these records at the end of each year and allocate a further retention period, or, SECURE DISPOSAL
6.2.6	Pupils' work	No		Where possible, work should be returned to the pupil at the end of the academic year. If this is not the school's policy, then current year + 1 year	SECURE DISPOSAL

7. Extracurricular Activities

7.1 Educational Visits outside the Classroom					
	Basic file description	**Data Protection Issues**	**Statutory Provisions**	**Retention Period [Operational]**	**Action at end of administrative life of the record**
7.1.1	Records created by schools in order to obtain approval to run an educational visit outside the classroom – Primary schools	No	Outdoor Education Advisers' Panel National Guidance website http://oeapng.info specifically Section 3 – "Legal Framework and Employer Systems" and Section 4 – "Good Practice".	Date of visit + 14 years	SECURE DISPOSAL
7.1.2	Records created by schools in order to obtain approval to run an educational visit outside the classroom – Secondary schools	No	Outdoor Education Advisers' Panel National Guidance website http://oeapng.info specifically Section 3 – "Legal Framework and Employer Systems" and Section 4 – "Good Practice".	Date of visit + 10 years	SECURE DISPOSAL
7.1.3	Parental consent forms for school trips where there has been no major incident[27]	Yes		Conclusion of the trip	Although the consent forms could be retained for date of birth + 25 years, the requirement for them being needed is low and most schools do not have the storage capacity to retain every single consent form issued by the school for this period of time

[27] One-off or blanket consent: The Department for Education (DfE) has prepared a one-off consent form to be signed by the parent on enrolment of their child in a school. This form is intended to cover all types of visits and activities where parental consent is required. The form is available on the DfE website for establishments to adopt and

7.1 Educational Visits outside the Classroom					
	Basic file description	**Data Protection Issues**	**Statutory Provisions**	**Retention Period [Operational]**	**Action at end of administrative life of the record**
7.1.4	Parental permission slips for school trips – where there has been a major incident	Yes	Limitation Act 1980 (Section 2)	Date of birth of the pupil involved in the incident + 25 years The permission slips for all the pupils on the trip need to be retained to show that the rules had been followed for all pupils	
7.1.5	Records relating to residential trips	Yes		Date of birth of youngest pupil involved + 25 years	SECURE DISPOSAL

7.2 Walking Bus					
	Basic file description	**Data Protection Issues**	**Statutory Provisions**	**Retention Period [Operational]**	**Action at end of administrative life of the record**
7.2.1	Walking bus registers	Yes		Date of register + 3 years. This takes into account the fact that, if there is an incident requiring an accident report, the register will be submitted with the accident report and kept for the period of time required for accident reporting	SECURE DISPOSAL [If these records are retained electronically any back up copies should be destroyed at the same time]

adapt, as appropriate, at www.gov.uk/government/publications/consent-for-school-trips-and-other-off-site-activities. A similar form could be used for other establishments, such as Early Years Foundation Stage (EYFS) providers and youth groups, or at the start of programmes for young people.

8. Central Government and Local Authority (LA)

This section covers records created in the course of interaction between the school and the LA.

8.1 Local Authority					
	Basic file description	**Data Protection Issues**	**Statutory Provisions**	**Retention Period [Operational]**	**Action at end of administrative life of the record**
8.1.1	Secondary transfer sheets (Primary)	Yes		Current year + 2 years	SECURE DISPOSAL
8.1.2	Attendance returns	Yes		Current year + 1 year	SECURE DISPOSAL
8.1.3	School census returns	No		Current year + 5 years	SECURE DISPOSAL

8.2 Central Government					
	Basic file description	**Data Protection Issues**	**Statutory Provisions**	**Retention Period [Operational]**	**Action at end of administrative life of the record**
8.2.1	OFSTED reports and papers	No		Life of the report then REVIEW	SECURE DISPOSAL
8.2.2	Returns made to central government	No		Current year + 6 years	SECURE DISPOSAL
8.2.3	Circulars and other information sent from central government	No		Operational use	SECURE DISPOSAL

Appendix A Glossary

Admissions Policy

Academies are their own admission authority (although the LA or another organisation can be contracted to carry out the tasks associated with the role). The Admissions Policy must comply with the requirements of the admission code and must be reviewed and adopted annually, irrespective of any changes. A formal consultation for a period of at least eight weeks between 1 November and 1 March must be carried out where any changes are required. Admissions-related information should be uploaded to the academy website.

Accessibility Plan

A plan or strategy must be put into place, setting out how disabled pupils can participate in the curriculum and associated services, thereby maximising access to both the physical environment and written information provided to pupils.[28]

Annual Report and Accounts

It is a condition of the funding agreement that Academy accounts must be produced for the 12-month accounting period ending on 31 August. The Annual Report and Accounts must be filed with Companies House by 31 May and should include the following elements:

Reports:

- A trustees' report;
- A governance statement;
- A statement on regularity, propriety and compliance;
- A statement of trustees' responsibilities;
- An independent auditor's report on the financial statements; and
- An independent auditor's report on regularity.

- Financial statements:
- A statement of financial activities;
- A balance sheet;
- A cash-flow statement; and
- Notes which expand on the statements, including a note on the Academy trust's accounting policies.[29].

Annual Return

Every Academy must file a completed annual return at Companies House each year.[30]

Articles of Association

The Articles of Association prescribe the internal management, decision-making and running of the Academy trust as well as its liability. The DfE has model documentation which schools are expected to adopt.[31]

Annual Report – Trustees'/Directors' Report

The Directors of the Academy are responsible for the preparation of a Trustees'/Directors' report which supports the financial statements. The report fulfils the requirements for a Directors' report, as set out in ss. 415–419 CA 2006, as well as a Trustees' report under charity law, as set out in the Charities' SORP. The main objective is to supplement financial information with such further information as necessary for a full appreciation of the company's activities. The report describes what the Academy is trying to do and how it is going about it, demonstrates whether and how the Academy has achieved its objectives during the year, and explains its plans for the future.[32]

Charging and Remissions Policy

An Academy is treated in the same way as a maintained school in respect of charging, particularly in relation to, charges, regulations about information about charges and school hours, voluntary contributions, recovery of sums as civil debt, interpretation regarding charges, and the obligation to enter pupils for public examinations. The terms also place an obligation on an Academy to have a Charging and Remissions policy.

The Education Act 1996 provides that parents and pupils cannot be charged for any activity, unless there is a policy in place. Charges per pupil cannot exceed the actual costs incurred, so that no extra cost can be charged to cover pupils who cannot afford the activity or in order to make a profit.

28 Paxton-Doggett, Katie "How to Run An Academy School" (ICSA 2014) p229.
29 *Ibid* p174.
30 *Ibid* pp68-69.
31 *Ibid* pp49ff.
32 *Ibid* p175

Charges for activities taking place during the normal school day can only be on the basis of voluntary contributions and pupils will be treated no differently whether they pay the contribution or not.

Directors – Appointment

The method of appointment will depend on the category of Director and the terms of the Articles. However, there must be at least two parent governors and no more than a third of Directors – including the Head Teacher – can be Academy staff. Directors are generally appointed for a term of 4 years.

Directors – Disqualification

The Company Directors' Disqualification Act 1986 grants the court power to make an order disqualifying a person from promoting, forming or taking part in the management of a company without the leave of the court. There are numerous grounds for disqualification and the model articles set out specific instances which will be regarded as disqualification.

Directors – Termination of Office

Generally, Directors are appointed for a fixed term of office, which in the model articles is set at 4 years. A Director may resign by giving written notice to the clerk at any time, although the articles provide that this will only be valid if there are at least three Directors remaining in office when the notice of resignation is to take effect. The Companies Act 2006 provides that a "company may by ordinary resolution at a meeting remove a director before the expiration of his period of office, notwithstanding anything in any agreement between it and him". This very wide provision is slightly tempered by the model articles, which state that Directors can generally be removed from office by the person or persons who appointed them. This means that where Directors are appointed by the members they can be removed from office, following a member resolution, by written notice to the clerk. Elected Directors cannot be removed in this way.

Funding Agreement with the Secretary of State

The Funding Agreement is effectively the contract by which the Academy agrees to provide educational services in exchange for funding provided by the DfE. There are model versions of the Funding Agreement, but these have been updated over time to reflect changes in policy and legislation. The DfE does not expect schools to deviate from the model documents.

Funding Records – Capital Grant

Specific prior written agreement by the Secretary of State must be obtained prior to incurring any capital expenditure on which capital grant payments are sought. Capital expenditure may include costs for building new premises or for substantially refurbishing existing premises.

Funding Records – Earmarked Annual Grant (EAG)

The EAG may be paid for either recurrent expenditure or capital expenditure for such specific purposes as have been agreed between the Secretary of State and the Academy. EAG may only be spent in accordance with the terms, conditions and scope of the grant, which are set out in the relevant funding letter.

Funding Records – General Annual Grant (GAG)

The GAG will be paid to cover the normal running costs of the Academy, such as salary and administration costs. The funding is equivalent to that which would be received by a maintained school with similar characteristics, together with an additional element for functions which would be carried out by the LA if the Academy were a maintained school.

General Members' Meetings

Meetings of the members are known as General Meetings. Apart from any specific requirement to call an Annual General Meeting, the Articles contain no specific obligations with regard to holding General Meetings. This means that it is feasible for long periods of time to pass without any meetings being held, since all resolutions are passed using the written resolution method! Members' meetings are closely regulated and the Companies Act 2006 has a whole chapter (Part 13, Chapter 3) dedicated to the requirements. This can be contrasted with Board Meetings, which have very little in the way of formal requirements.

Governance Statement

Academies are recipients of public funding and so must prepare a Governance Statement – this is a requirement by HM Treasury for all public bodies. It must be signed by the Chair and Accounting Officer on behalf of the board.

Memorandum of Association

Document confirming the three 'subscribers' who wish to form the Academy and become its members. The memorandum has no ongoing significance once an Academy has been incorporated.

Rules and Bylaws

The Directors are entitled to make "such rules or bylaws as they may deem necessary or expedient or convenient for the proper conduct and management of the Academy" in connection with matters that are "commonly the subject matter of company rules", such as in connection with meetings or members.

Special Educational Needs

The Academies Act 2010 provides that academies must have regard to the SEN Code of Practice. Published by the DfE, the Code of Practice includes adoption of a policy on SEN which sets out the approach to meeting pupils' special educational needs whether with or without a statement.

Strategic Review

Academies are now required to produce a strategic report, which must contain a fair review of the Academy's business as well as a description of the principal risks and uncertainties it faces. It will specifically include the following: achievements and performance; financial review; plans for future periods; and funds held as a custodian trustee on behalf of others. The Directors/Trustees must include a clear statement that they are approving the strategic report in their capacity as Company Directors.

Written Scheme of Delegation

The board can delegate any power or function to an individual Director, a committee, the principal or any other holder of an executive office. That person must report to the board when that authority has been exercised and any action taken, or decision made.