connecteducationtrust.org

CONNECT EDUCATION TRUST

Management of Records Guidance

Academic Year 2022-2025

Management of Records Guidance

Connect Education Trust recognises that by efficiently managing its records, it will be able to comply with its legal and statutory obligations and to contribute to the effective overall management of the Trust.

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

Information and Guidance

This information and guidance notes applies to all records created, received or maintained and stored by staff in the course of carrying out its functions.

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

A small percentage of the Trust's records may be selected for permanent preservation i.e. historical research.

Most records have retention periods, which can differ based on the type of data processed, the purpose of processing or other factors. Personal data should only be retained for as long as necessary. Issues to consider include:

- Whether any legal requirement apply for the retention of any particular data.
  For example:
  - Trade law
  - Tax law
  - Employment law
  - Administrative law

- In the absence of any legal requirements, personal data may only be retained as long as necessary for the purpose of processing. This means data is to be deleted e.g. when:
  - The data subject has withdrawn consent to processing and the data was collected on a consent basis
  - A contract has been performed or cannot be performed anymore; or
  - The data is no longer up to date

- Has the data subject requested the erasure of data or the restriction of processing?
- Is the retention still necessary for the original purpose of processing?

Responsibilities

The Trust has a responsibility to ensure it maintains its records and record keeping systems in accordance with the regulatory environment. The person with overall responsibility for this is the Headteacher of each school and the CEO.

The person responsible for records management will give guidance about good records management practice and will promote compliance, 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. Each school in the Trust will review annually their Data Handling Checklist for Compliance and Best Practice, emailing a copy of the checklist to the Trusts DPO, as evidence that the Trust are GDPR compliant.

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 Trusts records management guidelines 'Information Management Toolkit for Schools (IRMS)'. They must also have an overview of where personal data is stored:

- Own servers
- Third party servers
- Email accounts
- Desktops
- Employee – owned device (BYOD)
- Backup storage; and /or
- Paper files

Relationship with Existing Policies

This guidance and information has been drawn up within the context of:

- Freedom of Information Policy
- Data Protection Policy
- Other legislation or regulations (including audit, equal opportunities and ethics affecting the school).

Guidance on Pupil Records

All of our schools are under a duty to maintain a pupil record for each pupil. Early Years settings will have their own record keeping requirements.

The 'Pupil Record', comprised of educational and curriculum records, 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.

Managing Pupil Records

The pupil record is the core record charting an individual pupil's progress through the school. It will accompany them to every school they attend and will contain information that is accurate, objective and easy to access. A pupil or their nominated representative has the legal right to see their file at any point during their education and until the record is destroyed (when the pupil is 25 years of age or 35 years from date of closure for pupils with special educational needs). All information is accurately recorded, objective in nature and expressed in a professional manner.

Recording and Disclosure of Information

Pupil records may be held in paper form, or else electronically e.g. as part of the school management information system (MIS). Schools 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 two possible routes:

1. A request for an educational record. The Education (Pupil Information) (England) Regulations 2005, states that the pupil record must be provided to parents within 15 school days of a request where the pupil is enrolled in a maintained school. This provision does not apply to Academies, independent schools etc.
2. Requests for information by pupils, or their parents are to be treated as subject access requests (SARS) 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
- Admission 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 although this is not necessary if easily accessible through the MIS:

- 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. SEN, speech and language therapist, etc.
- Reference to any other linked files

Items which are included in the pupil record:

- Record of transfer from Early Years setting (if applicable)
- Admission for (application form)
- Data Collection/Checking Form – current (This should be checked regularly by parents to ensure details are accurate)
- National Curriculum and Religious Education locally agreed syllabus record sheets
- Fair processing notice
- Parental permission for photographs to be taken
- Years record
- Annual written report to parents *
- Any information relating to a major incident involving the child *
- Any reports written about the child *
- Any information about a statement and support offered in relation to the statement **
- Any relevant medical information *
- Child protection reports/disclosures are stored in a separate CP filing cabinet with a note to this effect on the pupil record
- Any information relating to exclusions (fixed or permanent) *
- Examination Results – pupil copy (Send uncollected certificates back to exam board after all reasonable efforts to contact the pupil have been exhausted)
- SATS Results (A note of the result should be recorded)
- Any correspondence or reference to correspondence with parents or outside agencies relating to major issues

- Details of any complaints made by the parents or the pupil are stored in the Headteachers office and a note to this effect on the pupil record.

*these are stored separately and securely on the school's management information system
** these are stored separately and securely in a SEN file

The following records should be stored separately to the pupil record as they are subject to shorter retention periods.

- Attendance Registers and Information
- Medicine consent and administering records (this is the school's record)
- Copies of birth certificates, passports, etc.
- Absence notes
- Parental consent for trips/outings
- Generic correspondence with parents about minor issues
- Accident forms (these should be stored separately and retained on the school premises until their statutory retention period is reached. A copy could be place on the file in the event of a major incident).
- Pupil work, drawings, etc.
- Previous data collection forms, now 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. The MIS 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.

The school is responsible for retaining the pupil record until the pupil reaches the age of 25 years. This retention is set in line with the Limitation Act 1980 which allows that a claim can be made against an organisation by a minor for up to 7 years from their 18th birthday.

The pupil record should be disposed of in accordance with the safe disposal of records guidelines.

If the school is requested to transfer a pupil file outside the EU area because a pupil has moved into that area, the school will contact the LA for further advice.

Storage and Security

Pupil records are kept securely at all times. Paper records are kept in lockable storage areas with restricted access and the contents are secure within the file. Electronic records also have appropriate security. Not everyone in a school has a need to access all of the information held about a pupil; this is particularly relevant to child protection information.

Access arrangements for pupil records ensure that confidentiality is maintained whilst equally enabling information to be shared lawfully and appropriately, and to be accessible for those authorised to see it.

If a member of staff requires the file to be removed from the secure room a signed record of the file removal should be obtained (signed out and signed back in).

Transferring Pupil Records

It is vital to ensure swift transfers of information to the new school 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, in which case these can be removed and securely destroyed.

Transfer Process

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

- Common Transfer File (CTF) from the MIS via the S2S system.
- Any elements of the Pupil Record, held in any format, not transferred as part of the CTF.
- SEND or other support service information, including behaviour, as only limited information will 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 school.

Schools 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, they 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 email, or other secure transfer method.

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

If a request is received to transfer the Pupil Record or other information about a pupil to a school outside of the United Kingdom (UK), schools should contact the Local Authority or their Data Protection Officer for further advice.

Retention and Disposal

Retention - Transferring school

Responsibility for maintaining the Pupil Record passes to the next school. Schools may wish to retain the information about the pupil for a short period to allow for any queries or reports to be completed, or where linked records in the MIS 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.

Please note: 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 that, at the conclusion of the inquiry, an

indication will be given regarding appropriate retention periods for child protection records. More information can be found on the IICSA website. The inquiry has now completed its public hearings, and has defined that information to be retained is limited to that relating to open investigations, currently Child Protection in religious organisations and settings, Allegations involving Lord Janner, and Residential Schools.

Retention – Last known school

The last known or final school is responsible for retaining the Pupil Record. The school is the final or last known school if:

- A secondary phase and the pupil left at 16 years old or for post-16 or independent education, or;
- It is a school 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.

During the retention period:

- Establish periodical reviews of data retained
- Establish and verify retention periods for data considering the following categories:
    - The requirements of our business
    - Type of personal data
    - Purpose of processing
    - Lawful grounds for processing; and
    - Categories of data subjects
- Establish periodical reviews of data retained

Digital Continuity

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

Where possible, these records should be "archived" to dedicated server space which is being backed up regularly. Where this is not possible the records could 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 must not be used to store these records as they are 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, used as appropriate. Software formats should be reviewed on an annual basis to ensure usability and to avoid obsolescence.

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. 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.

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, these 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.

Management & Monitoring of Electronic Communications

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.

All electronic communications, whilst they are held, are disclosable under Freedom of Information and Data Protection legislation. Be aware that anything staff write in an email, 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 the school to risk if used badly.

Messaging: Texts, Instant Messaging

Text messaging and IM applications can 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 email, telephone or delivered face-to-face. Avoid sending and posting sensitive/personal data as these systems may not be as secure as email.

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 etc.) 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 Freedom of Information 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 to say; 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 a school's Safeguarding and PREVENT obligations and the user's right to privacy. It will be important to include this in the appropriate policy 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 provide staff with advice on how you expect them to use systems such as email, 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 email and internet, that the logging is an appropriate record, and that it suits your policy.

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 school's requirements.

The Information Commissioner's Employment Practices Code is an excellent resource to use when considering this area:

https://ico.org.uk/media/for-organisations/documents/1064/the_employment_practices_code.pdf

What You Need to Know About Social Media

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 school 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 school is engaging with.

The school must ensure that staff contributors maintain the school's standards for written communications on Social Media platforms. Changes to Social Media tools are fast-paced and so 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, as 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 school to ensure consistent use of Social Media and that staff do not release information inappropriately or illegally.

Schools 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 school 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 schools 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 school 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 school 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 school 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 school 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 Act 2000 or under the Data Protection Act 2018 – they will also form part of the child or subject's digital footprint - clear and unambiguous consent is therefore key.

Social Media is disclosable under the access to information regimes

Both the Freedom of Information Act 2000 and Data Protection Act 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.

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 school messages/posts.
- Always sign off with a name (and school 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 spell check 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 school 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.

Appendix A

GOOD PRACTICE FOR MANAGING E-MAIL

1. Introduction

These guidelines are intended to assist you to manage e-mails in the most effective way, and must be used in conjunction with the Trusts policies on the use of ICT.

Information about how your e-mail application works is not included in this document.

2. **Eight Things You Need to Know About E-mail**

E-mail has replaced telephone calls and memos as communicating by e-mail is quick and easy, many people have replaced telephone conversations and memos with e-mail discussions. However, the language in which e-mail is written is often less formal and more open to misinterpretation than a written memo or a formal letter. Remember that e-mail should be laid out and formulated to the Trusts standards for written communications.

E-mail is not always a secure medium to send confidential information therefore you need to think about information security when you send confidential information by e-mail. The consequences of an e-mail containing sensitive information being sent to an unauthorised person could be a fine from the Information Commissioner or it could end up on the front page of a newspaper. Confidential or sensitive information should only be sent by a secure encrypted e-mail system. Never put personal information (such as a pupil's name) in the subject line of an e-mail.

Choose your recipients

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

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

Ensure that Bcc is used where appropriate to avoid the unauthorised disclosure of email addresses of intended recipients. (Note: the ICO has taken enforcement action in cases where Bcc has not been used in sensitive cases.)

E-mail is disclosable under the access to information regimes

All Trust e-mails are disclosable under Freedom of Information and Data Protection legislation. Be aware that anything you write in an email could potentially be made public.

E-mail is not necessarily deleted immediately E-mails can remain in a system for a period of time after you have deleted them. You must remember that although you may have deleted your copy of the e-mail, the recipients may not and therefore there will still be copies in existence. These copies could be disclosable under the Freedom of Information Act 2000 or under the GDPR Regulations 2018.

E-mail can form a contractual obligation

Agreements entered into by e-mail do form a contract. You need to be aware of this if you enter into an agreement with anyone, especially external contractors. Individual members of staff should not

enter into agreements either with other members of staff internally or with external contractors unless they are authorised to do so.

E-mail systems are commonly used to store information which should be stored somewhere else.

All attachments in e-mail should be saved into any appropriate electronic filing system or printed out and placed on paper files.

Employers must be careful how they monitor e-mail.

Any employer has a right to monitor the use of e-mail provided it has informed members of staff that it may do so. Monitoring the content of e-mail messages is a more sensitive matter and if you intend to do this you will need to be able to prove that you have the consent of staff. If you intend to monitor staff e-mail or telephone calls you should inform them how you intend to do this and who will carry out the monitoring. The Information Commissioner's Employment Practices Code is an excellent guide to this subject.

E-mail is one of the most common causes of stress in the work-place.

While e-mail can be used to bully or harass people, it is the sheer volume of e-mail which often causes individuals to feel that they have lost control of their e-mail and their workload. Regular filing and deletion can prevent this happening.

Creating and sending e-mail

Here are some steps to consider when sending e-mail.

Do I need to send this e-mail? Ask yourself whether this transaction needs to be done by e-mail? It may be that it is more appropriate to use the telephone or to check with someone face to face.

Who do I need to send this e-mail to? Limit recipients to the people who really need to receive the e-mail. Avoid the use of global or group address lists unless it is absolutely necessary. Never send on chain e-mails.

Use a consistent method of defining a subject line.

Having a clearly defined subject line helps the recipient to sort the e-mail on receipt. A clear subject line also assists in filing all e-mails relating to individual projects in one place. For example, the subject line might be the name of the policy, or the file reference number.

Ensure that the e-mail is clearly written

- Do not use text language or informal language in school e-mails.
- Always sign off with a name (and contact 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 a whole e-mail in capital letters.
- Always spell check an e-mail before you send it. Do not use the urgent flag unless it is absolutely necessary, recipients will not respond to the urgent flag if they perceive that you use it routinely.
- If possible, try to stick to one subject for the content of each e-mail, as it will be easier to categorise it later if you need to keep the e-mail.

Secure your data

The consequences of an email containing sensitive information being sent to an unauthorised person could result in sanctions or even a fine from the Information Commissioner, along with adverse publicity for the school. Confidential or sensitive information should be sent by a secure encrypted email or data transfer system. Never put personal information (such as a pupil's name) in the subject line of an email.

Sending attachments

Sending large attachments (e.g. graphics or presentations) to a sizeable circulation list can cause resource problems on your network. Where possible put the attachment in an appropriate area on a shared drive and send the link round to the members of staff who need to access it.

Disclaimers

Adding a disclaimer to an e-mail mitigates risk, such as sending information to the wrong recipient, or helps to clarify the school's position in relation to the information being e-mailed. Typically, they cover the fact that information may be confidential, the intention of being solely used by the intended recipient, and any views or opinions of the sender are not necessarily those of the Trust.

There is some debate about how enforceable disclaimers are. Legal advice should be sought when using or drafting a disclaimer for your organisation to ensure it meets your specific needs.

Managing received e-mails

This section contains some hints and tips about how to manage incoming e-mails.

Manage interruptions

Incoming e-mail can be an irritating distraction. The following tips can help manage the interruptions.

- Turn off any alert that informs you e-mail has been received
- Plan times to check e-mail into the day (using an out of office message to tell senders when you will be looking at your e-mail can assist with this).

Use rules and alerts

By using rules and alerts members of staff can manage their inbox into theme-based folders. For example:

- E-mails relating to a specific subject or project can be diverted to a named project folder
- E-mails from individuals can be diverted to a specific folder
- Warn senders that you will assume that if you are copied into an e-mail, the message is for information only and requires no response from you.
- Internally, use a list of defined words to indicate in the subject line what is expected of recipients (for example: "For Action:", FYI:", etc)
- Use electronic calendars to invite people to meetings rather than sending e-mails asking them to attend

Using an out of office message

If you check your e-mail at stated periods during the day you can use an automated response to incoming e-mail which tells the recipient when they might expect a reply. A sample message might read as follows:

Thank you for your e-mail. I will be checking my e-mail at three times today, 8:30am, 1:30pm and 3:30pm. If you require an immediate response to your e-mail please telephone me on xxxxxxxxx.

This gives the sender the option to contact you by phone if they need an immediate response.

Filing e-mail

Attachments only

Where the main purpose of the e-mail is to transfer documents, then the documents should be saved into the appropriate place in an electronic filing system or printed out and added to a paper file. The e-mail can then be deleted.

E-mail text and attachments

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 email in .msg format. This can be done either by clicking and dragging the e-mail into the appropriate folder in an application such as MS Outlook, or by using the "save as" function to save the e-mail in an electronic filing system.

If the e-mail needs to be re-sent it will automatically open into MS Outlook.

Where appropriate the e-mail and the attachments can be printed out to be stored on a paper -le, however, a printout does not capture all the audit information which storing the e-mail in .msg format will.

E-mail text only

If the text in the body of the e-mail requires filing, the same method can be used as that outlined above. This will retain information for audit trail purposes.

Alternatively, the e-mail can be saved in a pdf format. This will save all the text in the e-mail and a limited amount of the audit information. The e-mail cannot be re-sent if it is saved in this format.

The technical details to undertake all of these functions are available in application Help functions.

Disclaimer

Adding a disclaimer to an email can mitigate 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 school. However, legally it is likely that these are not enforceable, but at the very least they can help clarify the school's position in relation to the information being emailed.

Look out for Phishing!

Make sure staff are aware of the dangers of providing information over email. Never provide passwords or personal data, or click on a link in an email without verifying its source. Ask your IT department to provide advice.

How long to keep e-mails?

E-mail is primarily a communications tool, and e-mail applications are not designed for keeping e-mail as a record in a storage area meeting records management storage standards.

An 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? Safeguarding? Or Child Protection?

The retention for keeping these e-mails will then correspond with the Trusts retention Policy.

Appendix B

INFORMATION SECURITY AND BUSINESS CONTINUITY

Information Security and Business Continuity are both important activities in ensuring good information management and are vital for compliance with the data protection law. Taking measures to protect our Trust records can ensure that:

- You can demonstrate compliance with the law and avoid data loss incidents;
- In the event of a major incident, your school should be able to stay open and will at least have access to its key
- Administrative and teaching records.

Your Business Continuity Plan and should deal with records held in all media across the Trusts systems:

- Electronic (including but not limited to databases, word processed documents and spreadsheets, scanned images)
- Hard copy (including but not limited to paper files, plans)
- Hard copy (including but not limited to paper, files, plans)

Digital Information

In order to mitigate against the loss of electronic information a school needs to:

- **Operate an effective back-up system**

You should undertake regular backups of all information held electronically to enable restoration of the data in the event of an environmental or data corruption incident. Where possible these backups should be stored in a different building to the servers and if possible off the main school site. This is to prevent loss of data, reduce risk in case of theft or the possibility of the backups becoming temporarily inaccessible. Options for the management of back-up facilities include:

- **Use of an off-site, central back up service** (usually operated by another provider).

This involves a backup being taken remotely over a secure network (usually overnight) and stored in encrypted format in premises other than the school.

- **Storage in a fireproof or bombproof safe in another part of the school premises**

The back-up may be stored in a fireproof safe which is located in another part of the premises. These premises must be also be physically secure and any hard copy supporting data regarding the location of records should also be stored in the safe.

- **Control the way data is stored within the Trust**

Personal information must not be stored on the hard drive of any laptop or PC unless the device is running encryption software. Staff should be advised not to hold personal information about students or other staff on mobile storage devices including but not limited to memory sticks, phones, iPads, portable hard drives or even on CD.

- **USB Flash Drives**

Personal information must not be stored on USB Flash Drives

- **Maintain strict control of passwords**

Ensure that the data is subject to a robust password protection regime, preferably with mandatory multi-factor authentication. Users should change passwords periodically and use the NCSC “three

words" guidance for forming passwords. Password sharing is not permitted; use alternative ways for users to share data – like shared network drives or proxy access to email and calendars. In addition, staff should always lock their devices when they are away from the desk to prevent unauthorised use.

- **Manage the location of server equipment**

Ensure that the server environment is managed to prevent access by unauthorised people.

- **Ensure that business continuity plans are tested**

Test restore processes routinely to ensure that the first time you identify a problem with the backup is not the first time you need to retrieve data from it.

For advice on preserving information security when using email see the fact-sheet on good practice for managing email.

Hard Copy Information and Records

Records which are not stored on the School/Trusts servers are at greater risk of damage by fire and flood as well as risk of loss and of unauthorised access.

- **Fire and flood**

The cost of restoring records damaged by water can be high but a large percentage can be saved, fire is much more destructive of records. In order to limit the amount of damage which a fire or flood can do to paper records, all vital information should be stored in filing cabinets, drawers or cupboards. Metal filing cabinets are a good first level barrier against fire and water.

Where possible vital records should not be left on open shelves or on desks as these records will almost certainly be completely destroyed in the event of fire and will be serious damaged (possibly beyond repair) in the event of a flood.

- **Unauthorised access, theft or loss**

Personal data held in paper form is kept in locked cabinets and is only Taken off Trust premises with the permission of the Chief Executive Officer (CEO) or the Headteacher, on the understanding that it be securely stored.

All archive or records storage areas should be lockable and have restricted access. Personal data should always be locked away at the end of every day and should not be left visible on desks, noticeboards, etc… at any time.

Personal data held on a computer must be encrypted and regularly backed up if it is not duplicated elsewhere.

Personal information must be kept in a locked filing cabinet, drawer or safe.

Child Protection records are kept in a locked cabinet – access is restricted to the Designated Child Protection Officer/ Senior Leadership Team
Laptops and computers are password protected

Sensitive data should never be stored off site

Disclosure

Personal information is not disclosed either orally or in writing or via Web pages or by means, accidently or otherwise, to any unauthorised third party.

Staff should note that unauthorised disclosure will usually be a disciplinary matter, and may be considered gross misconduct in some cases.

Risk Analysis

The Trusts Risk Management Policy ensures the Trust has a consistent basis for measuring, controlling, monitoring and reporting risk across the Trust at all levels.

Individual schools and departments within the Trust should identify which records are vital to school management and these records should be stored in the most secure manner.

Responding to Incidents

In the event of an incident involving the loss of information or records contact the Trusts Data Protection Officer (DPO) of in her absence the Chief Operations Officer, who will pull together an incident response team to manage the situation.

Major Data Loss/Information Security Breach

If there is a major data loss or information security breach. This will involve contacting the Data Protection Officer (DPO) or in their absence the DCEO/CFO, who will liaise with the Information Commissioner's Office if an information security breach needs to be reported.

Fire/Flood Incident

Follow the Emergency Plan procedures.

Appendix C

SAFE DISPOSAL OF RECORDS

NB: Please be aware that this guidance applies to all types of record, whether they are in paper or electronic form.

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 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.

Disposal of records that have reached their minimum retention schedule

Records should be kept no longer than necessary.

In each school records that are no longer required for business use are reviewed as soon as practicable under the criteria set out so that ill – considered destruction is avoided.

The review will determine whether records are to be selected for permanent preservation, destroyed, digitised to an electronic format or retained by the Trust for research or litigation purposes.

Managing Records Retention

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.

Each school should have a designated staff member with responsibility for ensuring records are retained, reviewed and destroyed in accordance with requirements, and as soon as possible once their lifespan has expired. They will need to 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 record-keeping system or a manual system.

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 record keeping systems.

Refer to the trust's retention policy (Appendix D- Retention Guidelines at the bottom of this document)

Safe destruction of records

All records containing personal information, or sensitive policy information should be made either unreadable or unreconstructable:

- Paper records should be shredded using a cross-cutting shredder
- 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

All non – personal records should be bundled up and disposed of to a waste paper merchant or disposed of in other appropriate ways.

Do not put records in with the regular waste or a skip.

There are companies who can provide confidential waste bins and other services which can be purchased to ensure that records are disposed of in an appropriate way.

a) Where an external provider is used

It is recommended that all records must be shredded on-site in the presence of an employee. A secure area must be designated where records can be stored prior to shredding.

The organisation must also be able to prove that the records have been destroyed by the company who should provide a Certificate of Destruction. Staff working for the external provider should have been trained in the handling of confidential documents.

The shredding needs to be planned with specific dates and all records should be identified as to the date of destruction. It is important to understand that if the records are recorded as to be destroyed but have not yet been destroyed and a request for the records has been received they MUST still be provided.

b) Where records are destroyed internally

The process must ensure that all records are recorded are authorised in accordance with guidelines and by the Headteacher/ HR Officer/ Office Manager. All records should be shredded by two persons as soon as the record has been documented as being destroyed, and logged on the GDPR Audit Asset spreadsheet.

c) Where records are destroyed externally 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 schools 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 schools 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

Approved contractors should always provide a Certificate of Destruction, which should be retained with details of individual records destroyed.

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 school'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 to the type of information. The school's ICT department or IT provider should be able to advise on the most appropriate method.

The 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).

Transfer of Information to Other Media

Where lengthy retention periods have been allocated to records, the school may wish to consider converting paper records to 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 to 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. Schools/Trust must 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 six months after transfer to an alternative media, so as to provide adequate time in which any issues arising out of the data transfer process may be identified.

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 Freedom of Information Act 2000 requires schools and Academies to maintain a list of records which have been destroyed and a record of who authorised their destruction. The Act states that, as a minimum, the school should be able to provide evidence that the destruction of records took place as part of a routine records management process. Schools must assess whether they are creating another piece of Personal Identifiable Information (PII) by maintaining a record of evidence, particularly if they are listing the names of the people whose records have been deleted.

Freedom of Information Act 2000 (FOIA 2000)

The Freedom of Information Act 2000 requires the school to maintain a list of records which have been destroyed and who authorised their destruction.

Members of staff should record at least:

- File reference (or other unique identifier);
- File title (or brief description);
- Number of files and date range
- The name of the authorising officer
- Who is destroying the data
- Date action taken
- Reference to the applicable retention period
- 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)

Following this guidance will ensure that the school is compliant with the GDPR Regulations and the Freedom of Information Act 2000.

3. Transfer of records to the Archives

Where records have been identified as being worthy of permanent preservation, arrangements to be made by the Trust to archive i.e. historic information about the school.

4. Transfer of information to other media

Where lengthy retention periods have been allocated to records, members of staff may wish to consider converting paper records to other media such as microform or digital media. 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 to electronic media. It is essential to have procedures in place so that conversion is done in a standard way. This means that schools can prove that the electronic version is a genuine original and

could not have been tampered with in any way. Reference should be made to 'British Standard 10008:2008 'evidential weight and legal admissibility of electronic information' when preparing such procedures.

Recording of all archiving, permanent destruction and digitisation of records

Sample appendices are provided for the recording of all records to be used. These records could be kept in an Excel spreadsheet or other database format.

Appendix D – https://irms.org.uk/page/SchoolsToolkit

(IRMS) Toolkit for Schools - currently there isn't a separate Records Retention Schedule for Academies.

Additional Trust Retention Periods:

Volunteers – Retention period current year plus 6 years

Emails – Retention period 3 years