Dunmow St Mary's Records Management Policy

Responsibilities for management of information to support secure access and effective retention, destruction and preservation processes

Policy points are numbered. The numbering corresponds to explanations of 'why?' and 'how?' for each point further down the page.

What must I do?

1. ***MUST***: You must **document** your work activities in line with procedures
2. ***MUST***: You must store all work information in the format and **medium** best suited to its use in line with procedures
3. ***MUST***: You must ensure that the information you manage is only known to an **appropriate audience**
4. ***MUST***: All information in any format which we hold as a record of our activity must be **retained** after 'closure' in line with our Retention Guidelines.
5. ***MUST***: Owners must regularly **review** information in line with Retention Guidelines to make best use of the available storage space.
6. ***MUST***: We must **monitor** the success of the review process to maintain compliance with the law
7. ***MUST***: You must manage Pupil records in line with the school's procedures (Appendix A) and specific system **guidance**
8. ***MUST***: You must follow Good Practice for Managing E-mail (See Appendix B) when storing **emails** as records
9. ***MUST***: We must ensure that the **facilities** available for storing and managing information meet legal requirements and best practice.
10. ***MUST***: We must maintain a **selection procedure** for identifying, reviewing and managing records with **historical value**
11. ***MUST NOT***: You must not store business information on a **personal drive** or on equipment not provided by the Organisation
12. ***MUST***: All Information **Assets** identified on the Register must be associated with a retention period from the Retention Guidelines.
13. ***MUST***: The Retention Guidelines must be reviewed for **changes** in legislation and the Organisation's business needs.
14. ***MUST:*** When archiving paper records, information on ownership, retention and indexing quality must be recorded.
15. ***MUST NOT:*** You must not use the archive storage services of any other commercial company than the **approved supplier**

Why must I do it?

- These measures ensure Organisation information, where appropriate to do so, is shared effectively to support efficient business processes and maintain effective service delivery to customers.
- Managing records in line with the best practice guidance fulfils duties under the section 46 Code of Practice on Records Management under the Freedom of Information Act 2000. Retention Guidelines are published so there is clear communication to customers over what information should still be available to them if they wish to make a request. To retain information too long or to destroy too soon leaves us open to criticisms on openness and transparency, and in some cases, compliance with the law.

- In order to comply with the Section 46 Code of Practice (see above) we must ensure that we are destroying all related information across all formats. For example, destroying a paper file on a project but keeping all the electronic documents about the project in a shared network folder can cause problems if a Freedom of Information request is received. The request co-ordinator assumes that as the paper file is destroyed then we do not hold any information and responds accordingly. We would then be in breach of the act.

How must I do it?

1. Employees are aware of best practice requirements and any guidance on use of specific systems through training and communications
2. Employees are aware of best practice requirements and any guidance on use of specific systems through training and communications
3. You must ensure that paper files are accessible to authorised colleagues in your absence, by ensuring others know where to find keys to lockable storage areas. You must be aware of who information should be shared with, and ensure it is only shared with that audience. You must ensure that you save electronic information in a shared environment, but with appropriate access controls if the information has a restricted audience.
4. Follow the best practice guidance and any superseding amendments made by the Organisation
5. Follow the best practice guidance and any superseding amendments made by the Organisation
6. Designated employees must gather performance data on activities within the scope of this policy for review by the Data Protection Officer and the Leadership Team
7. Follow the best practice guidance and any superseding amendments made by the Organisation
8. Follow the best practice guidance and any superseding amendments made by the Organisation
9. The organisation must approve and regular review facilities such as systems and physical storage as appropriate against security requirements in Data Protection Law, and all employees must help maintain security standards by following procedure.
10. Records can be identified for preservation at any point in the records lifecycle, but will not transfer until we have no ongoing administrative need (i.e. at the end of a retention period). When information is due to be destroyed, there should be a final review to select records for transfer to the Essex Record Office.
11. By only storing all business information on the relevant systems designated by the Organisation and by using only equipment approved by the Organisation.
12. The Information Asset Owner is responsible for ensuring that Information Asset Managers amend entries on the Information Asset Register to show the correct retention period from the schedule.
13. A policy review (at least annually) must review the provisions of best practice retention guidance and make any necessary amendments, documenting the reasons for change and managing affected records accordingly.
14. We must complete and retain archiving indexes providing the relevant information about paper records in storage, ensuring that the Organisation is aware of what information it holds at all times and when they can be reviewed.
15. Any use of a commercial storage provider must be assessed and approved to ensure the right security and financial provisions are place. Use of alternatives that have not been approved may not provide value for money and may not provide secure services.

What if I need to do something against the policy?

If you believe you have a valid business reason for an exception to these policy points, having read and understood the reasons why they are in place, please raise a formal request by contacting Clare Griffiths, Senior Information Risk Officer.

Document Control

Version: 1

Date approved: 24th April 2018

Approved by: Dunmow St Mary's Primary School

Next review: 24th April 2021

References

- Data Protection Act 1998 (to May 25th 2018)
- General Data Protection Regulations 2016 (from 25th May 2018)
- Article 8, The Human Rights Act 1998
- Freedom of Information Act 2000.
- Code of Practice on Records Management (under Section 46 of the FoIA)

Breach Statement

Breaches of Information Policies will be investigated and may result in disciplinary action. Serious breaches of Policy may be considered gross misconduct and result in dismissal without notice, or legal action being taken against you.

Appendix A – School's guidelines for storing Pupil Records (Best Practice)

Pupil Records at DSM

These guidelines apply to both physical and electronic records.
All pupils arriving at DSM have a paper file created with key personal information. This information is also stored on our MIS. The paper files are stored in a locked filing cabinet within the secure office area. The electronic files are protected by password access.

Pupil records are transferred when the child leaves the school e.g. move to secondary school. Custody of and responsibility for the records passes to the school the pupil transfers to.

Files are only sent by post where absolutely necessary. These are sent by registered post with the record of postage retained by the school. Where possible files are hand delivered and signed for to say that they have been received.

There are some exceptions to this which are described in the school's retention schedule.

Appendix B – Good Practice for Managing Email.

1. Introduction

These guidelines are intended to assist school staff to manage their e-mail in the most effective way, and must be used in conjunction with your school's 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 your school's standards for written communications.

E-mail is not always a secure medium to send confidential information. 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 civil penalty of up to £500,000 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.

E-mail is disclosable under the access to information regimes. All school e-mail is 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 Data Protection Act 1998.

E-mail can form a contractual obligation. Agreements entered into by e-mail can 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 Whilst e-mail can be used to bully or harass people, it is more often the sheer volume of e-mail which causes individuals to feel that they have lost control of their e-mail and their workload. Regular filing and deletion can prevent this happening.

3. 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.

To whom do I need to send this e-mail? 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. When sending emails containing personal or sensitive data always respond to an authorised, approved address. All emails that are used for official business must be sent from an official business domain address.

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. This can be interpreted as shouting.
- 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.

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 school. 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.

4. Managing received e-mails

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

a) 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).

b) 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 in to 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

c) 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.

5. 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 e-mail 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 file, 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 .html or .txt 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 about how to undertake all of these functions are available in application Help functions.

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. 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? The retention for keeping these e-mails will then correspond with the classes of records according to content in the retention schedule for schools found elsewhere in the Records Management Tool Kit for Schools. These e-mails may need to be saved into any appropriate electronic filing system or printed out and placed on paper files.

Acknowledgements Original Content developed by: Suzy Taylor New College Durham Anthony Sawyer Herefordshire Public Services John Davies TFPL Consultancy Minor amendments made by the editor in the 2015 Review