Smithy Street Primary School

Data Protection Policy

Part 2 Record Management

APPROVED BY STAFF AND GOVERNORS
JANUARY 2016

The School recognises that the efficient management of its records is necessary to comply with its legal and regulatory obligations and to contribute to the effective overall management of the institution. This document provides the policy framework through which this effective management can be achieved and audited. It covers:

- Scope
- Responsibilities
- Relationships with existing policies

Scope of the policy

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

1.2 Records are defined as all those documents which facilitate the business carried out by the school 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.

1.3 A small percentage of the school's records will be selected for permanent preservation as part of the institution's archives and for historical research.

2 Responsibilities

2.1 The school 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 School.

2.2 The person responsible for records management in the school will give guidance for good records management practice and will promote compliance with this policy so that information will be retrieved easily, appropriately and timely.

2.3 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 school's records management guidelines.

3 Relationship with existing policies

This policy has been drawn up within the context of:

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

Contents:

Information Security

Information security is an integral part of the Data Protection Act 1998. Staff must take all reasonable steps to ensure that any personal or sensitive information which they are collecting and storing is securely stored.

You will find below some guidelines to bear in mind when considering information security:

1. All personal information should be kept in lockable filing cabinets which are kept locked when the room is unattended. Personal information should not be left on your desk where anyone could see it. You might need to consider restricting access to offices in which personal information is being worked on or stored.

2. If you are “archiving” information somewhere else in your own building (or in an outbuilding) make sure that the door can be locked and that the key is kept locked away. Anyone accessing the room should sign for the key. Where possible, there should be a file tracking system where anyone borrowing items from the “archive” room must make a note of what they have taken.

3. Personal information held on computer systems should be adequately password protected. Information should never be left up on a screen if the computer is unattended. Make sure that you don’t have shared passwords to systems (or share personal passwords with other members of staff) and that all members of staff log off the computer when it is left unattended.

4. Where possible personal information should not be sent by e-mail, as its security cannot be guaranteed. Using a “safe haven” fax is preferable to e-mail (a fax machine in a secure or constantly manned area). Never send personal information in the text of an e-mail, if necessary make sure that the information is in an MSOffice document attached to the e-mail. When sending land-mail through either the internal or external postal system make sure that the information is in a sealed envelope.

5. When using children or other members of staff to transport personal information around the school make sure that the information is in an envelope or a file.

6. If files need to be taken off the premises they should be secured in a lockable box or briefcase and put in the boot of the car. Any items containing personal information (e.g. laptops, PDAs, briefcases etc) should not be left in a car on open view. Records should not be left in the boot of a car overnight or for any extended period of time. Once you have taken the records from the car please make sure that they are not left on general access in your home. Put them out of sight in a secure environment.

7. If using a home computer (or laptop) to process personal information ensure you have up-to-date virus protection software installed. No other members of your household should have access to the computer or the information contained on it. Any documents produced should be stored onto disk and not to the hard drive.

8. Be careful of giving out personal information over the telephone; invite the caller to put the request in writing. If the request is urgent take the callers name and switchboard telephone number and verify their details before responding.

9. Do not discuss other people's personal business in public areas where conversations can be overheard by people with no right to know the details of the information.

One of the best rules of thumb for dealing with sensitive, personal information, is to ask the question "if this was my information would I be happy with the way in which it is being treated?"

The best ways of disposing of sensitive, personal information are dealt with in the section looking at the disposal of records.

E-mail Management

Table of Contents

1. Introduction

These guidelines are intended to assist members of staff to manage their e-mail in the most effective way.

2. Ten Things to Remember About E-mail

2.1 E-mail is a vehicle to carry information

There is a commonly held myth that e-mail should be treated differently to other methods of transporting information. The important thing to remember is that e-mail is the vehicle by which we transport information. It is the same as an envelope, a fax machine or a telephone. We don’t talk about how we deal with an envelope, or a fax machine or a telephone, we only consider the information which we have received via these means. E-mail is no different.

Try viewing e-mail as the tool rather than an end in itself and see if this changes the way which you manage your e-mail.

2.2 E-mail has replaced the telephone as a main means of communication

As communicating by e-mail is quick and easy, many people have replaced telephone conversations with e-mail discussions. As a result the language in which e-mail is written is less formal and can be more open to misinterpretation than a written memo or a letter on headed note paper.

Members of staff need to remember that e-mail should be laid out and formulated to KCC’s standards for written communications.

Members of staff may need to consider whether the issue under discussion could be dealt with by a phone call or even in a face to face discussion.

2.3 E-mail can be misinterpreted

In a normal face to face communication, most information is exchanged in an environment where the participants can read the body language of the person they are speaking to. They can assess the value of the words the person is saying in combination with a facial expression or tone of voice.

Over the telephone, the two participants can assess the words they are hearing against the tones of voice being used in the exchange of words. In both face to face and telephone communication the participants can ask for clarification about things they don’t understand and move the conversation forward.

An e-mail conversation only contains the words written by the sender. These may be open to misinterpretation (some humour works in an e-mail context, most of it doesn’t). Members of staff need to bear this in mind when they are creating e-mails (see section 3 below).

2.4 E-mail is not a secure medium to send confidential information

E-mail which is sent via the web can be routed via a number of different ISPs, which may be hosted in a number of different countries. Even on the secure internal e-mail system e-mail can be mis-sent.

Members of staff need to think about information security issues when they decide to 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. Other information, if mis-sent, could end up on the front page of a newspaper.

If at all possible, confidential or sensitive information should not be sent by e-mail.

2.5 E-mail is disclosable under the access to information regimes

As e-mail is used for all types of correspondence there is the danger that people phrase e-mails more informally than they would other documents such as memos. All e-mail is disclosable under Freedom of Information and Data Protection legislation.

Any personal information which is contained in a work e-mail (e.g. about holidays, health, family situations) may become disclosable with the rest of the e-mail. Where possible members of staff should try not to include personal details in e-mails which contain information relating to work matters.

2.6 E-mail is not completely deleted immediately

Although the “deleted” box is emptied as you exit MS Outlook, e-mails can remain in the system for a period of time after that. Where e-mail is journalled or archived the e-mail can be kept for up to a year (as required by the Counter-Terrorism Act 2000). Members of staff need to remember that whilst they may have deleted their copy of the e-mail, the recipient (and the people to whom the recipient has forwarded it to) may not and therefore there will still be a copy in the system. These copies could still be disclosable under the Freedom of Information Act 2000 or under the Data Protection Act 1998.

2.7 E-mail can form a contractural obligation

Agreements entered into by e-mail do form a contract. Members of staff need to be aware of this if they 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.

2.8 E-mail systems are commonly used to store core information inappropriately

It is a commonly held statistic that if there is no formal way of declaring e-mail as a record then up to 80% of the organisation's core information could be held within the e-mail system. All attachments and core information should be saved into the appropriate electronic filing systems or printed out and placed on paper files.

2.9 Employers have a right to monitor e-mail

Members of staff should be aware that any employer has a right to monitor use of e-mail provided it has informed members of staff that it may do so. An organisation has this right because it has a vicarious liability in all the actions of its employees (for example, if a member of staff has been sending material of an inappropriate nature to other colleagues or members of the public, then the organisation may be found liable for any damage or distress caused).

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

E-mail is cited as being one of the most common causes of stress in the work-place. E-mail can be used to bully or harass employees but it is commonly the sheer volume of e-mail which causes individuals to feel that they have lost control of their e-mail and their workload. Consistent e-mail management can prevent this happening.

3. Creating and sending e-mail

There are five different steps in this section which members of staff can consider when creating and sending e-mail. The way in which e-mail is created can impact the whole course of the e-mail conversation.

3.1 Do I need to send this e-mail?

Ask the question, "does this transaction need to be done by e-mail?". It may be that it is more appropriate to use the telephone or to check with some one face to face.

3.2 Who do I need to send this e-mail to?

Limit the recipient list 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. Having to type in addresses or pick addresses from the global address list is time-consuming but it focuses the sender on exactly who needs to receive the e-mail.

3.3 Use a consistent method of defining a subject line

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

3.4 Ensure that the e-mail is clearly written

Make sure that the e-mail is written in a way which reflects that this is a written medium of communication.

- Do not use text language or informal language where this is not appropriate.
- Always start the e-mail with a greeting and sign off with a name (and contact details). The sign off may be separate from your automatic signature.
- Make sure that you use plain English in the e-mail and ensure that you have made it clear how you need the recipient to respond. This will enable the recipient to respond more quickly.
- Never write a whole e-mail in capital letters. In e-mail terms this is the equivalent of shouting at someone. Never use a red coloured text as this can convey danger or warning (unless red is part of the corporate colour scheme for communications and this is understood by the recipient)
- Never write an "angry" e-mail. Write the e-mail, go away and leave it, and then come back and re-read it as though you were the recipient.
- Ensure that you read the e-mail through as though you were the recipient to ensure that you have made yourself clear and always spell check the e-mail before you send it. Remember that the person receiving the e-mail will form an impression of you from that e-mail that may make a difference to the way in which they respond to you.
- 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.

3.5 Sending attachments

Sending large attachments (e.g. graphics or presentations) to a sizeable circulation list can cause considerable storage problems on a network server (especially if everyone keeps a copy of the e-mail in their inbox). 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.

4. Managing received e-mails

Managing in-coming e-mails can be one of the more stressful aspects of the process as the member of staff has no control over the e-mails which other people choose to send them. This section contains some hints and tips about how to manage incoming e-mails.

4.1 Managing Interruptions

Incoming e-mail can be an irritating distraction and can also become addictive (constantly looking to see what e-mail has arrived). The following tips can help manage the interruptions.

- Turn off any form of automatic flag that e-mail has been received (e.g. the noise or visual reminder)
- 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) and then check e-mail only at those times.

4.2 Use rules and alerts

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

- All Extramail can be diverted to a named folder
- E-mails relating to a specific subject or project can be diverted to a named project folder (this tends to rely on the sender using the agreed subject lines)
- E-mails from individuals can be diverted to a specific folder

This allows e-mail to be managed in themed sections and can also allow recipients to weed out e-mails which are of less importance.

4.3 Limit subscriptions to list-serves/distribution lists

Only subscribe to the professional or service specific list-serves and distribution lists that are absolutely necessary. It may also be possible to view the posts to a list via a web site periodically rather than have them sent as e-mail to your inbox.

5. Replying to e-mails

E-mail reaches its destination so quickly that there is sometimes a danger that the recipient requires an immediate response. There are some tips below about how to control this.

5.1 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 (much as you do when you are away from your desk for any period of time). 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 01622-69xxxx.

This gives the sender the option to contact you by phone if they need an immediate response, otherwise the e-mail can be fed into your normal work-flow.

5.2 Managing your e-mail responses

The following hints are designed to help manage e-mail responses:

- Sort the e-mail in the inbox, either by the urgent flag or by the name of the person who sent it or by the subject line or by the date it was received;
- Scan each e-mail for content and then decide what to do with it (it is necessary to at least take a cursory glance at each e-mail in case you miss something important before you prioritise them);
- Sort out the e-mail in those which can be dealt with immediately (i.e. responses to meetings, items that can be answered immediately). There is no point in double-handling the e-mail (then file or delete the e-mail);
- Prioritise the remaining e-mail (if you have used the rules and alerts outlined above some of

this prioritisation will already have been done for you, for example, all your Extramail may well be in one folder). This can be by simply using a folder structure in MS Outlook, High Priority, Medium Priority and Low Priority, and dragging the e-mail into the relevant folder.

- Work through the e-mail folders in order of priority. At this stage it may be appropriate to send an e-mail to the sender letting them know when you are likely to be dealing with their e-mail.

6. Managing the “sent” box

Managing the “sent” box can be a challenge especially if the sent items contain large attachments. Where it is necessary to keep “sent” items as part of an agreed audit trail, they should either be saved in to the appropriate folder in MS Outlook, or the appropriate folder in an electronic filing system (or printed out and filed in the paper file).

Where possible it is better that members of staff do not manage e-mail from within the “sent” box unless e-mail is retained in the “sent” box until a reply has been received and then it is deleted.

7. Filing e-mail

7.1 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.

7.2 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 the metadata 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 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 metadata which storing the e-mail in .msg format will.

7.3 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 in 7.2 above. This will retain the metadata 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 metadata.

The e-mail can not be re-sent if it is saved in this format.

The technical details to undertake all of these functions are available in MS Office Outlook Help.

Managing Pupil Records

The pupil record should be seen as the core record charting an individual pupil's progress through the Education System. The pupil record should accompany the pupil wherever they find themselves in the Education system and should contain information that is accurate, objective and easy to access.

1. File covers for pupil records

We use a consistent file cover for the pupil record.
By using pre-printed file covers all the necessary information is collated and the record looks tidy and reflects the fact that it is the principal record containing all the information about an individual child.

2. Recording information

A pupil or their nominated representative can ask to see their file at any point during their education (and indeed until they reach the age of 25 years when the record is destroyed). It is important to remember that all information should be accurate and objective and expressed in the appropriate language.

3. Primary School records

3a. Opening a file

The pupil record starts its life when a file is opened for each new pupil as they begin school. This is the file which will follow the pupil for the rest of his/her school career. The following information should appear in the file:

- Surname
- Forename
- DOB
- Gender
- Position in family
- Ethnic origin [although this is "sensitive" data under the Data Protection Act 1998, the DfES require statistics about ethnicity]
- Language of home (if other than English)
- Religion [although this is "sensitive" data under the Data Protection Act 1998, the school has good reasons for collecting the information]
- Names of parents and/or guardians with home address and telephone number
- Name of the school, admission number and the date of admission and the date of leaving.

Inside the front cover the following information should be easily accessible:

- The name of the pupil's doctor
- Emergency contact details

3b. Items which should be included on the pupil record

- If the pupil has attended an early years setting, then the record of transfer should be included on the pupil file

- Admission form (application form)
- Parental permission for photographs to be taken
- Annual Written Report to Parents
- Any information relating to a major incident involving the child (either an accident or other incident)
- Any reports written about the child
- Any information about a statement and support offered in relation to the statement
- Any relevant medical information (should be stored in the file in an envelope)
- Child protection reports/disclosures (should be stored in the file in an envelope clearly marked as such)
- Any information relating to exclusions (fixed or permanent)
- Any correspondence with parents or outside agencies relating to major issues
- Details of any complaints made by the parents or the pupil

3c. Transferring the pupil record to the secondary school

The pupil record should not be weeded before transfer to the secondary school .It is important to remember that the information which may seem unnecessary to the person weeding the file may be a vital piece of information required at a later stage.

Primary schools do not need to keep copies of any records in the pupil record except if there is an ongoing legal action when the pupil leaves the school. Custody of, and therefore responsibility for, the records passes to the school the pupil transfers to.

If files are sent by post, they should be sent by registered post with an accompanying list of the files. Where possible, the secondary school should sign a copy of the list to say that they have received the files and return that to the primary school. Where appropriate records can be delivered by hand.

4. Responsibility for the pupil record once the pupil leaves the school

The school which the pupil attended until statutory school leaving age (or the school where the pupil completed sixth form studies) 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 minor for up to 7 years from their 18th birthday.

5. Safe destruction of the pupil record

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

6. Transfer of a pupil record outside the EU area

If you are requested to transfer a pupil file outside the EU area because a pupil has moved into that area, please contact the Local Education Authority for further advice.