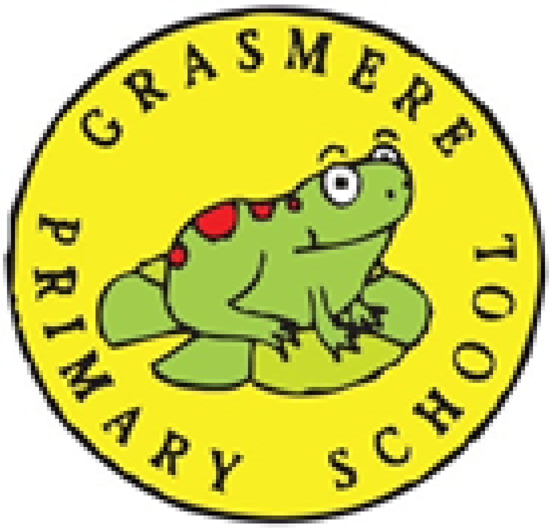

GRASMERE PRIMARY SCHOOL

Records Management Policy and Guidance

Revised: May 2018

Review Date: May 2020

Contents

Policy p3

Guidance p4

Pupil Records p4

Introduction p4
Primary School Records p4-5
Responsibility for the pupil record once the pupil leaves the school p6
Safe Destruction of Pupil Records p6
Transfer of a Pupil Record outside the EU Area p7
Storage of Pupil Records p7

Information Audits p7

What is an information audit? P7
Benefits of an information audit p8
How to conduct an information audit p8

Good Practice for Managing Email p9
Introduction p9
Steps to consider when sending emails p9-10
Managing received emails p10
Filing emails p11-12

Safe Disposal of Records p12
Disposal of records that have reached the end of the minimum retention period allocated p12
Safe destruction of Records p12-13
Transfer of records to the Archives p13
Transfer of information to other media p14
Retention Guidelines p14
The purpose of the retention guidelines p14
Benefits of a retention schedule p14
Maintaining and amending a retention schedule p15

Information Security and Business Continuity p15
Digital Information p15
Hard Copy Information and Records p16
Disclosure p17
Risk Analysis p17
Responding to Incidents p18

Policy

1. Scope of the policy

1.1 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.

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 based on the Grasmere Primary School Records Management Guidance and will promote compliance with this policy so that information will be retrieved easily, appropriately and in a timely way. They will also monitor compliance with this policy by surveying at least annually to check if records are stored securely and can be accessed appropriately.

2.3 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

. GDPR 2018

. And with other legislation or regulations (including audit, equal opportunities and ethics) affecting Grasmere Primary School.

Guidance

Pupil Records

Introduction

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 to every school they attend and should contain information that is accurate, objective and easy to access.

Pupils have a right of access to their educational record and so do their parents under the Education (Pupil Information) (England) Regulations 2005. Under the GDPR 2018 a pupil or their nominated representative has a right to see information held about them. This right exists until the point that the file is destroyed. Therefore, it is important to remember that all information should be accurately recorded, objective in nature and expressed in a professional manner.

Primary School Records

Files should be created and stored electronically or in hard copy. The following information should be included when opening a file for a pupil:

- Surname
- Forename(s)
- DOB
- Unique Pupil Number

The following information should be included when opening a file, and updated if appropriate:

- Date when file was created (and if appropriate, when file closed)
- The name of the pupil's doctor
- Emergency contact details
- Gender
- Preferred name
- Position in family
- Ethnic origin
- Home language (if other than English)
- Religion
- Any allergies or other medical conditions that it is important to be aware of
- Names of adults who hold parental responsibility with home address, telephone numbers and email as appropriate, and any additional relevant carers and their relationship to the child

- Name of the school, admission number and the date of admission (and date of leaving where appropriate)
- Any other agency involvement, e.g. speech and language therapist, paediatrician

It is essential that these files, which contain personal information, are managed against the information security guidelines.

Additional items which should be part of the pupil record

Some of the following items may be stored in separate secure areas within the school, e.g. Safeguarding and Child Protection reports. If this is the case, a note must be kept with the record to indicate information is stored separately for this pupil.

- 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)
- Privacy Notice [if these are issued annually only the most recent need be on the file]
- Photography Consents
- Medical and Dietary Needs Consents
- 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 or Education Health Care Plan and support offered in relation to the statement
- Any relevant medical information
- Safeguarding or Child protection reports/disclosures
- 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

The following records should be stored separately to the pupil record as they are subject to shorter retention periods and if they are placed on the file then it will involve a lot of unnecessary weeding of the files before they are transferred on to another school.

- Absence notes
- Parental consent forms for trips/outings (in the event of a major incident all the parental consent forms should be retained with the incident report, not in the pupil record)
- 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 placed on the pupil record file in the event of a major incident)

Transferring the pupil record to the secondary school

The pupil record should not be prepared before transfer to the secondary school unless any records with a short retention period have been placed in the file. It is important to remember that the information which may seem unnecessary to the person preparing the file may be a vital piece of information required at a later stage.

Any records kept separately should be added to the file, and in the case of relevant medical information or child protection reports/disclosures should be stored in the file in a sealed envelope clearly marked with name of pupil and type of information.

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 responsibility for the records passes to the school the pupil transfers to.

Files should not be sent by post unless absolutely necessary. If files are sent by post, they should be sent by registered post with an accompanying list of the files. 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 with signed confirmation for tracking and auditing purposes.

Electronic documents that relate to the pupil file also need to be transferred, or, if duplicated in a master paper file, destroyed.

Responsibility for the pupil record once the pupil leaves the school

The school which the pupil attended until statutory school leaving age (raised to 18 in 2015) is responsible for retaining the pupil record until the pupil reaches the age of 25 years. (See the ***retention schedule*** for further information).

Safe destruction of the pupil record

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

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 Authority for further advice.

Storage of pupil records

All pupil records should be kept securely at all times. Paper records, for example, should be kept in lockable storage areas with restricted access, and the contents should be secure within the file. Equally, electronic records should have appropriate security.

Access arrangements for pupil records should 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.

Information Audits

What is an information audit?

- An information audit is a form of records survey encompassing:
- Paper documents and records
- Electronic documents and records
- Databases (proprietary or developed in-house)
- Microfilm/microfiche
- Sound recordings
- Video/photographic records (including those records taken on traditional magnetic tape and photographic paper but increasingly digital sound, video and photo files)
- Hybrid files (including both paper and electronic information)
- Knowledge

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

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

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

Benefits of an information audit

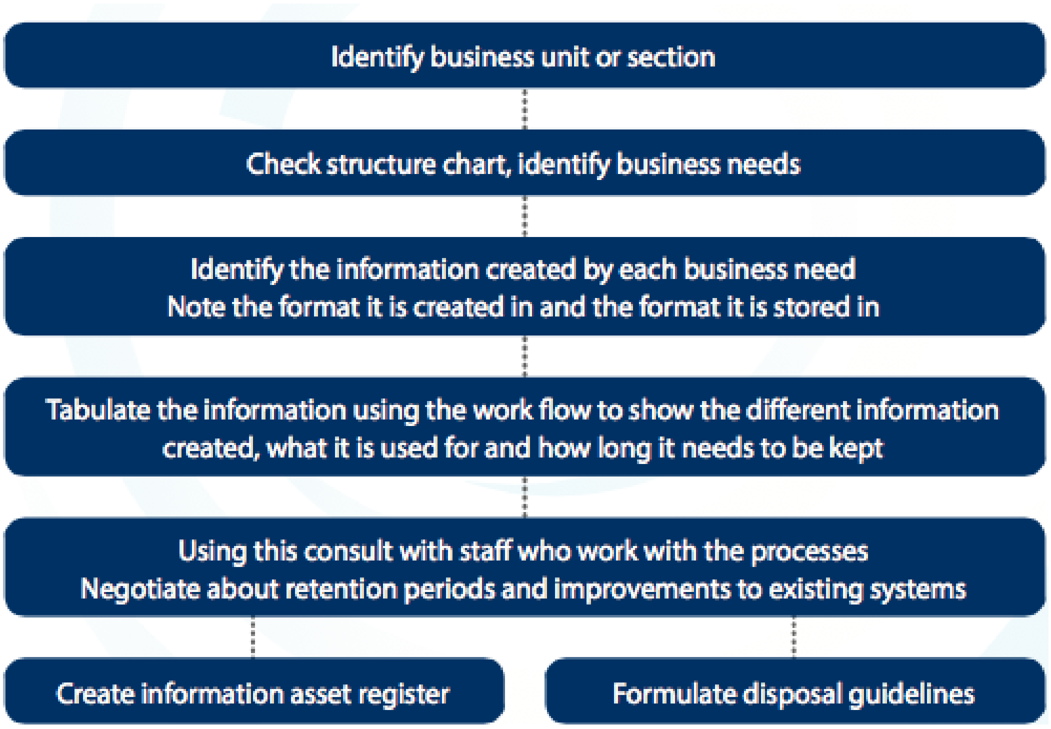
An information audit collects the information necessary to formulate and implement an efficient records management programme and to ensure compliance with legislation. It is designed to allow organisations to discover the information they are creating, holding, receiving and using and therefore to manage that information in order to get the most effective business use from it. For a school the concept is much more concerned with accessibility of information.

The information audit allows the school to identify the personal information it creates and stores to allow correct management under the GDPR 2018 (Under the GDPR all schools, whether they are Local Authority Controlled, Academies or part of the independent sector are Data Controllers in their own right).

Information a school creates and uses to make the decisions which affect people's daily lives may well become subject to the Freedom of Information Act 2000. Grasmere Primary School uses the publication scheme included within the Trust's Freedom of Information policy and scheme.

How to Conduct an Information Audit

The IRMS Toolkit for Schools suggests a procedure (relevant sections on pp14-16) for conducting an information audit based on the following flowchart:


Identify business unit or section
Check structure chart, identify business needs
Identify the information created by each business need
Note the format it is created in and the format it is stored in
Tabulate the information using the work flow to show the different information created, what it is used for and how long it needs to be kept
Using this consult with staff who work with the processes
Negotiate about retention periods and improvements to existing systems
Create information asset register
Formulate disposal guidelines

Source IRMS Toolkit for Schools

Good Practice for Managing Email

All Grasmere Primary School employees should ensure that emails include the following disclaimer at the foot of every email:

This message contains confidential information and is intended only for the individual named. If you are not the named addressee you should not disseminate, distribute or copy this e-mail. Please notify the sender immediately by e-mail if you have received this e-mail by mistake and delete this e-mail from your system. E-mail transmission cannot be guaranteed to be secured or error-free as information could be intercepted, corrupted, lost, destroyed, arrive late or incomplete, or contain viruses. The sender therefore does not accept liability for any errors or omissions in the contents of this message, which arise as a result of e-mail transmission. If verification is required please request a hard-copy version.

All school email is disclosable under Freedom of Information and Data Protection legislation.

Agreements entered into by email 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.

Email is one of the most common causes of stress in the workplace. Whilst email can be used to bully or harass people, it is more often the sheer volume of email which causes individuals to feel that they have lost control of their workload. Regular filing and deletion can prevent this happening.

Steps to consider when sending emails

Do I need to send this email?

Ask yourself whether this transaction needs to be done by email? 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 email?

Limit recipients to the people who really need to receive the email. Avoid the use of global or group address lists unless it is absolutely necessary. Never send on chain emails.

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 email on receipt. A clear subject line also assists in filing all emails relating to individual projects in one place.

Ensure that the email is clearly written

- Do not use text language or informal language in school emails.

- 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 email in capital letters. This can be interpreted as shouting.
- Always spell check an email 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 email, as it will be easier to categorise it later if you need to keep the 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.

Managing received emails

Manage interruptions

Incoming e-mail can be an irritating distraction.

- Turn off any alert that informs you email has been received
- Plan times to check email into the day (using an out of office message to tell senders when you will be looking at your email 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:

- Emails relating to a specific subject or project can be diverted to a named project folder
- Emails from individuals can be diverted to a specific folder
- Warn senders that you will assume that if you are copied in to an email, 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 emails asking them to attend

Using an out of office message

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

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

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

Filing emails

Attachments only

Where the main purpose of the email 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 email can then be deleted.

Email text and attachments

Where the text of the email adds to the context or value of the attached documents it may be necessary to keep the whole email. 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 email into the appropriate folder in an application such as MS Outlook or by using the “save as” function to save the email in an electronic filing system.

If the email needs to be resent it will automatically open into MS Outlook.

Where appropriate the email 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 email in .msg format will.

Email text only

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

Alternatively the email can be saved in .html or .txt format. This will save all the text in the email and a limited amount of the audit information. The email 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 emails?

Email is primarily a communications tool, and email applications are not designed for keeping email as a record in a storage area meeting records management storage standards.

Email 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 emails will then correspond with the classes of records according to content in the retention schedule for schools found elsewhere in this guidance. These emails may need to be saved into any appropriate electronic filing system or printed out and placed on paper files – although printing hard copies should be avoided unless necessary.

Safe disposal of records

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

Disposal of records that have reached the end of the minimum retention period allocated

The fifth data protection principle states that:

Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes

In each organisation, local records managers must ensure that records that are no longer required for business use are reviewed as soon as possible under the criteria set out so that only the appropriate records are destroyed. The local review will determine whether records are to be selected for permanent preservation, destroyed, digitised to an electronic format or retained by the organisation for research or litigation purposes.

Refer to the Retention Guidelines in this set of guidelines. Whatever decisions are made they need to be documented as part of the records management policy within the organisation.

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

- Any other 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 unless there is no other alternative. 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.
- Where an external provider is used it is recommended that all records must be shredded on-site in the presence of an employee. 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.
- Where records are destroyed internally, the process must ensure that all records are recorded are authorised to be destroyed by a Senior Manager and the destruction recorded. Records should be shredded as soon as the record has been documented as being destroyed.

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
- Date action taken

Following this guidance will ensure that the school is compliant with the Data Protection Act 1998 and the Freedom of Information Act 2000.

Transfer of records to the Archives

Where records have been identified as being worthy of permanent preservation arrangements should be made to transfer the records to the County Archives Service. The school should contact the local record office if there is a requirement to permanently archive the records, and the records will continue to be managed via the GDPR 2018 and the FoIA 2000. If you would like to retain archive records in a special archive room in the school for use with pupils and parents please contact the local record office for specialist advice.

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 organisations 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.

Retention Guidelines

The purpose of the retention guidelines

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

Members of staff are expected to manage their current record keeping systems using the retention schedule and to take account of the different kinds of retention periods when they are creating new record keeping systems.

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

Benefits of a retention schedule

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

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

Maintaining and amending a retention schedule

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

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

Some of the retention periods are governed by statute. Others are guidelines following best practice. Every effort has been made to ensure that these retention periods are compliant with the requirements of the GDPR 2018 and the Freedom of Information Act 2000.

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

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 GDPR 2018. Taking measures to protect your records can ensure that:

- Your school 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.

An Information Security Policy should incorporate a Business Continuity Plan and should deal with records held in all media across all school 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)

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 the local authority or other 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 data 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 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 school

Personal information should 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, and portable hard drives or even on CD.

Maintain strict control of passwords

Ensure that the data is subject to a robust password protection regime, ideally with users changing their passwords every 30 days. Discourage password sharing strongly and seek 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 PCs 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 on a regular basis 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.

Hard Copy Information and Records

Records which are not stored on the school’s 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 may 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 seriously damaged (possibly beyond repair) in the event of a flood. The bottom shelves of a storage cupboard should be raised at least 2 inches from the ground. Physical records should not be stored on the floor.

Unauthorised access, theft or loss

Staff should be encouraged not to take personal data on staff or students out of the school unless there is no other alternative. Records held within the school should be in lockable cabinets. Consider restricting access to offices in which personal information is being worked on or stored. All archive or records storage areas should be lockable and have restricted access. Where paper files are checked out from a central system, log the location of the file and the borrower, creating an audit trail.

Clear Desk Policy

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

Disclosure

Staff should be made aware of the importance of ensuring that personal information is only disclosed to people who are entitled to receive it. Ensure that where you intend to share personal information with a third party that you have considered the requirements of the Data Protection Act. Be careful of giving out personal information over the telephone; invite the caller to put the request in writing, supplying a return address which can be verified.

Where appropriate you may wish to develop a data sharing protocol with the third parties with whom you regularly share data.

Risk Analysis

Individual schools should undertake a business risk analysis to identify which records are vital to school management and these records should be stored in the most secure manner. Reference materials or resources which could be easily replaced are more suitable for storage on open shelves or desks.

The development of an information asset/risk register can assist with this process.

Responding to Incidents

In the event of an incident involving the loss of information or records the school should be ready to pull together an incident response team to manage the situation. Schools should consider assigning a specific member of staff to deal with press/media enquiries.

Major Data Loss/Information Security Breach

You should have a process which must be used by all members of staff if there is a major data loss or information security breach. This will involve appointing a named member of staff to liaise with the Information Commissioner’s Office if an information security breach needs to be reported.

Do not put off informing the Information Commissioner’s Office if the incident is serious enough to justify notification. It is better to have notified the Information Commissioner before someone makes a complaint to him.