

Freedom of information



KENT COUNTY COUNCIL
RECORDS MANAGEMENT TOOLKIT FOR SCHOOLS

Version 3: 17 July 2007



Data Protection &
Freedom of Information



Records Management Toolkit for Schools

The Records Management Toolkit for Schools has been created to assist schools in their compliance with the Freedom of Information Act 2000. The toolkit has been revised and some additions have been made. The information below outlines what can be found in the toolkit with links to the relevant documents which can then be downloaded and amended electronically for use in the school. If you have any comments to make about the Records Management Toolkit for Schools, or would like to suggest any additions, please contact Elizabeth Barber (Records Manager) on elizabeth.barber@kent.gov.uk.

Records Management Policy

Each public authority (including individual schools) should have a records management policy. The toolkit contains a [policy document](#) which can be adopted in its entirety or adapted to reflect the different needs of different schools.

Records Management Programme

The Records Management Toolkit aims to assist individual schools to manage records throughout their lifecycle. There is advice about [setting up filing systems](#) and creating records, including some basic questions to think about when creating records. There is advice about [managing e-mail](#) to ensure that it becomes part of the vital record. There is information and advice about [information security](#) and how to ensure compliance under the Data Protection Act 2000. There is also information about [business continuity](#) to ensure that vital records are not lost or destroyed in the event of fire, flood or theft. There is also some advice about how to conduct an [information audit](#).

Pupil Records

Some guidelines about what should be included in the main [pupil record](#) have been included and some advice about what information should be transferred on to the next school and how this information should be transferred.

Retention Guidelines

The core part of the toolkit are the [retention guidelines](#) which list all the possible records any school, anywhere in Kent, might produce and the recommended retention periods. Some of these have a statutory basis, others have been agreed in consultation with schools around the county. There is some information about the [benefits of using a retention schedule](#) there are also guidelines about the [safe disposal of records](#) including transferring records to Archive and Local History Services.

Closed School Guidance

There is some general guidance about needs to be done with records when [a school closes](#) or amalgamates with another school in the same area.

Training

If you are interested in getting some training about the Records Management Toolkit for Schools and about Data Protection and Freedom of Information please contact Michelle Hunt on michelle.hunt@kent.gov.uk.

Records Management Policy

Under section 6 of the Lord Chancellor's Code of Practice on the Management of Records under Section 46 of the Freedom of Information Act 2000:

An school should have in place an overall policy statement, endorsed by top management and made readily available to staff at all levels of the organisation, on how it manages its records, including electronic records.

The policy statement should provide a mandate for the performance of all records and information management functions. In particular, it should set out an school's commitment to create, keep and manage records which document its principal activities. The policy should also outline the role of records management and its relationship to the school's overall strategy; define roles and responsibilities including the responsibility of individuals to document their actions and decisions in the school's records, and to dispose of records; provide a framework for supporting standards, procedures and guidelines; and indicate the way in which compliance with the policy and its supporting standards, procedures and guidelines will be monitored.

The policy statement should be reviewed at regular intervals (at least once every three years) and, if appropriate, amended to maintain its relevance.

[For a full copy of the Lord Chancellor's Code of Practice see www.dca.gov.uk/foi/codesprac.htm]

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

The following is a model policy statement which could be adopted by individual schools. It has been extracted from *Model action plan for developing records management compliant with the Lord Chancellor's Code of Practice under Section 46 of the Freedom of Information Act 2000 Model Action Plan for Schools*.

For more information about the Records Management Policy please contact Elizabeth Barber on elizabeth.barber@kent.gov.uk.

[Name of] School

Records Management Policy

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

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.
- 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.

Creating Information Management Systems

1. Creating a new record keeping system

ISO15489 defines records as:

information created, received and maintained as evidence and information by an organisation or person, in pursuance of legal obligations or in the transaction of business.

Records can be stored in different ways, in a paper format, in electronic media or in microform format. The storage media makes no difference to the way in which the information is managed.

Information created by the school must be managed against the same standards regardless of the media in which it is stored. There is a common misconception that because the storage of electronic records is more cost effective than the storage of manual records, it is not necessary to manage this information against the same rigorous standards relating to manual systems. It is not acceptable to retain electronic information for longer periods of time.

Information management systems fall into three main categories:

- manual (i.e. paper or microform)
- electronic (digital information)
- hybrid (a mixed system of manual and electronic systems).

It is clear that in the short to medium term most schools will manage most of their information using hybrid systems. This is inevitable until the legal admissibility of electronic records is more clearly defined by case law¹. It can be extremely difficult to facilitate access to information under the freedom of information legislation using hybrid systems unless a strict classification rules are in operation. Otherwise, it will be impossible to be sure that all the information for a single request has been retrieved within the appropriate time frame.

Information management systems should be created using the business process as a model before records need to be created. If record keeping systems develop at the same time as the records themselves, any system is likely to be idiosyncratic and it will be harder to gain access to the information it contains. The information management system needs to be designed to reflect the business practice and workflow and should be flexible enough to be amended if the business practice changes. Staff can then be trained in the use of the system before any "filing" is undertaken.

2. Maintenance of record keeping systems

It is important that the process of filing information is properly resourced and is carried out on a regular basis. The information audit process may identify information which does not need to be retained. It is equally important that the files are weeded of extraneous information where appropriate on a regular basis. Removing information from a file once a freedom of information request has been made will be a criminal offence (unless it is part of normal processing), therefore the files need to be reviewed on a regular basis.

It may also be appropriate to remove paper-clips, elastic bands, post it notes and other accessories which can damage the file, when the file is weeded. It may also be appropriate to photocopy information which is on flimsy paper onto better quality paper to ensure its survival.

When members of staff are creating files it is useful to give some thought as to the length of time which a file will need to be operational. Using the retention schedule for this purpose can be

¹ See BIP0008:2004

useful. If a file is likely to be retained permanently (for example, it is of historical or legal value) it may be appropriate to use an archival quality paper to store the information on, to limit the use of post it notes on the text, to use brass paper clips or brass staples for securing papers, not to use sellotape to "mend" papers and not to use tippex on documents. All these precautions will extend the life of the file. Signed minutes, legal documents and other similar records would fall within this category.

However, it would be an over-reaction (not to mention expensive) to apply these rules to a finance file, for example, or general correspondence files which will be retained for much shorter periods of time.

Applying retention periods is straightforward provided files are closed on a regular basis. A number of criteria can be used to close a file:

- In the case of project files it would be usual to close each file cover when it becomes full and to close the whole project when it has been completed.
- In the case of administrative files, such as correspondence or finance, the files can be closed when the file cover becomes full or on an annual basis.
- In the case of files where there is very little action, files could be closed 5 years after the last action on the file.

Once a file has been closed it can be moved out of the current filing system and stored either in a record room in the school or in another appropriate place until it has reached the end of the retention period.

3 Using electronic systems

The purpose of any information management system needs to be clearly defined, together with the reasons for keeping the information. Legal admissibility issues need to be clearly defined. The length of time the information needs to be stored in the system also needs to be clearly defined.

A suitable system then needs to be chosen to meet the needs identified above. For example, in the case of information which needs to be retained for long periods of time, electronic systems are not ideal unless data migration issues are addressed when the system is set up.

The system which meets most of the business requirements identified above should be used wherever possible. If a manual solution is the best solution then it should be used above an electronic system. Storage space issues often force members of staff into opting for an electronic system where it is not completely appropriate.

Where possible the use of hybrid systems should be avoided as they are the most difficult to manage. A comprehensive system of cross-referencing needs to be used to ensure that all the relevant information can be extracted from both systems when it is required.

A file classification scheme needs to be created. Since the demise of the central filing registries, effective file classification schemes are not always created when new information management systems are introduced. Filing classification schemes are essential in order to ensure that information is filed consistently (for example, there are not five different files with the same information from different dates because five different people have done the filing) and in the case of hybrid systems it ensures that the electronic and manual information are kept together "intellectually" although they may be stored in different places.

The filing classification scheme should reflect the business process as far as possible. This makes the actual filing process much more simple. It may be necessary to adopt an alpha, numeric, or alphanumeric system which an MSWindows directory will support (i.e. the use of "-" or ".").

characters which would make good sense in a purely manual system can not be used in an electronic system).

Alpha-numeric systems which connect with the business process are generally easier for users to remember and use effectively.

Once the classification scheme has been agreed and documented it needs to be decided which documents in a process need to be captured into the file:

For example:

Should drafts be filed or just the final report?;

Should all copy correspondence be filed, or just that which adds to the record?

Should generic information supplied by third parties be automatically put on the file, and if so does the school have the agreement of the third party to release this information under freedom of information?

Having a list of the kind of documents which the business process is likely to produce helps in this process. Involving members of staff who are involved in the process on the front line is useful at this stage as they are the most appropriate people to assess what will be needed for operational purposes.

In the past members have staff have tended to file information "just in case". Under the freedom of information regime all this information will become subject to the Act and may need to be disclosed if a request is received. This could lead to much more work than is necessary. Equally, it is clear that some information has been disposed of much too early in its life-cycle which will be unacceptable under the Act. The capture of agreed information onto the file will ensure that all the information is being managed in a consistent manner.

Once the content of the different files have been determined an initial retention period needs to be allocated to them and the record series need to be added to the school retention schedule.

All of this information should be documented. Once this has been completed this process will become "normal processing" and provided members of staff follow the agreed and documented process they will be protected against any accusation of "tampering" with files once a freedom of information or data subject access request has been made.

These guidelines are intended to help members of staff manage their e-mail in the most effective way they can. In this way information communicated by e-mail can be filed and retrieved in the same way that all the other information received by members of staff.

1. Dispel the myth

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.

2. E-mail management

Part of the issue with e-mail is that people think that because they have sent you the information in the blink of an eye, they can expect the answer back within a similar time-frame, this puts pressure on people. Remember that you can always acknowledge receipt of an e-mail and give the sender a rough idea of when you will deal it (in the same way in which we use an acknowledgement card). If it's urgent they'll soon let you know.

Leaving lots of e-mails unread can cause a workflow problem. It is useful to open e-mails to see what they contain even if you don't deal with it immediately. How many times have we all been caught out at a meeting where we don't have the right information and the convener gaily announces they e-mailed it to you three weeks ago!

You can sort your e-mail in a number of ways in the in-box. For example, you can group all the urgent messages together and deal with them first, or you can group together all the e-mails from a particular person or on a particular subject and deal with them in order of importance. This can help you manage the e-mails in a structured way.

You can use your out of office message or an auto reply in a number of different creative ways. Your message can state that:

- You are out the office and when you are back and who the person should contact if they are sending a freedom of information request;
- You are engaged on another project and you will deal with the e-mail on a given day;
- You are presently taking "x" amount of time to deal with your e-mails and if the request is urgent could someone phone you;

and indeed in many other ways. This gives the sender an idea of how long you are likely to take to reply.

If a member of the public sends a freedom of information request the 20 working days begins when the e-mail arrives in your in-box. If your out of office message gives the message that you are out of the office and that the requestor needs to contact an alternative e-mail address then the clock stops either until you return or until the requestor contacts the person you have suggested.

If you have to forward an e-mail to someone else to deal with, it is a good idea to send a reply to the sender to tell them you have referred it on and who to contact if they have a query. This will save you being hassled by the sender when the person who should be dealing with it has failed to reply!

3. Managing e-mail into your workflow

In the same way that a huge pile of paper on your desk can seem a very daunting prospect so can a huge number of e-mails, especially on your return from leave or if you've been away from the office.

It is wise to open all your e-mail so that you know the scale of the issues you are dealing with. This is also wise if you find e-mails you need to forward, it is not helpful if they've sat in your box unread for three weeks when someone else could have dealt with them in half the time.

The following is one method of dealing with your e-mails as you open them. This method applies equally if you sort your e-mail list or if you leave it unsorted.

4. Saving and storing e-mail

4.1 *Pending e-mail*

If you have allocated the e-mail to your workflow system it should not remain in your in-box. There is a facility in MS Outlook to create "personal" folders. You can call these folders by the name of a project, by the days of the week when you intend to deal with them, by the name of the person in your team and so on.

E-mails should only remain in these folders whilst you are waiting to answer them or work on them. Once the transaction has been completed you need to make sure that the text of the e-mail and any attachments are filed (see 4.2 below).

For a diagrammatic representation of workflow to manage e-mail see Figure 1 below.

4.2 *Filing information communicated via e-mail*

The emphasis has now moved away from the "vehicle" to the information. You need to make a decision about whether the information should be captured as part of your record keeping system. Once you have made that decision you either delete the information in the e-mail or you file it in your main filing system in the appropriate place.

You can file the e-mail itself electronically into your electronic file plan:

- Select the e-mail and find save as on the file menu
- Save the e-mail as an outlook message format (.msg) using the agreed file naming conventions

This has the advantage of saving all the metadata from the e-mail (i.e. who sent it and when, who else was copied and so on). It also means that if necessary you can re-send the e-mail in its original format. If you save the e-mail in .msg format, all attachments will be saved attached to the e-mail.

If you need to save the attachments in to the electronic filing system independently of the e-mail text then you need to do the following.

- Right click on the attachment icon and save as to the appropriate file using the agreed file naming conventions.

This is useful if the e-mail is being used solely as a vehicle for transporting documents.

You may need to save either e-mail or attachments into a paper system:

- Print out the e-mail and attachments and file in the appropriate file.

Usually, by printing the document out you will lose all the metadata attached to the e-mail.

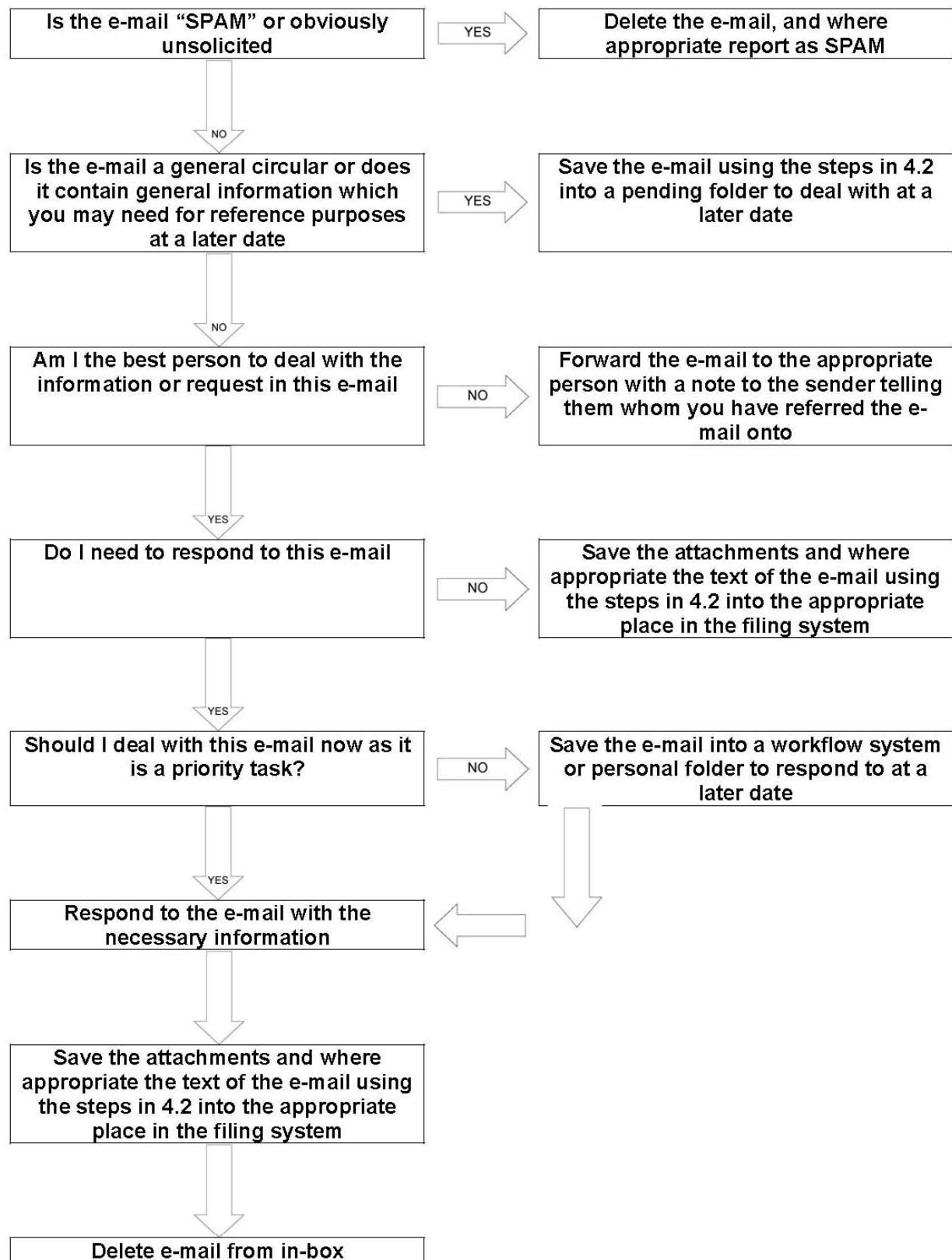
You can then delete the e-mail from your pending box.

4.3 *Managing sent e-mail*

If you have sent an e-mail to someone initiating a request for information then you should decide whether or not the e-mail you sent should be captured into the main filing system. If it should be captured then follow the steps outlined in 4.2 above.

There are occasions where you may need to prove that you sent an e-mail to a particular person on a particular day. There is no reason, however, why you need to keep all your sent e-mail in your sent e-mail box awaiting the "box full" message from ISG. This is especially true if there are huge attachments to your e-mail. Periodically, for example, daily, weekly, monthly . . . you should capture your sent e-mail into a file using the different techniques identified in 4.2.

Figure 1 E-mail management flow chart



Information Security

Information security is an integral part of the Data Protection Act 1998. You must take all reasonable steps to ensure that any personal or sensitive information which you 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.

If you need to know any more about information security please contact either Michelle Hunt (michelle.hunt@kent.gov.uk) or Elizabeth Barber (elizabeth.barber@kent.gov.uk)

Business Continuity

Business continuity is an integral part of managing records under both Data Protection Act 1998 and the Freedom of Information Act 2000. It is also important to ensure that if a major incident does occur then individual schools can stay open (in line with CFE policy) and ensure that all the information which is required is available.

There are two main areas where schools may be affected by business continuity issues:

1. Major computer failure (i.e. theft of computers or corruption of data)
2. Environmental incidents (i.e. fire or flood)

1. Major Computer Failure

Major computer failure can take two forms, but in both cases, a robust back up system is vitally important.

There are two areas of concern when computers are stolen. In the first place, the data on the computers (some of it sensitive personal data) could fall into the wrong hands and be misused by the individuals who have stolen the computers. Do not store sensitive personal information on the hard drives of either desk top or lap top computers unless absolutely necessary (e.g. you are taking a lap top home to work on data). All sensitive information should be stored on network drives where possible. If the server is on the school premises, ensure that the data is subject to a robust password protection regime and that the server is stored in a place which has adequate security.

If the electronic data becomes corrupted on the server then the school will need to ensure that they can restore the regular backups (see below).

The school should undertake regular backups of all information held electronically (see below) so that data can be installed on any new equipment which has been purchased or reinstalled once the corrupted data has been removed. Where possible these backups should be stored off the main school site. In the event of a fire (see 2 below) backups can be destroyed or corrupted along with other data (even if they are in a safe). It is also possible that the emergency services will not allow members of staff back on the site to pick up any backups for a number of days after any incident has occurred. In the case of theft if the safe is stolen along with the computers then the backups could be stolen along with the computers.

There are a number of different options which are available to schools to ensure that back ups are taken on a regular basis. It is also important to test periodically that backups can be restored. There have been occasions in the past where the first time a problem with the backup has been detected is when someone has tried to restore it after a major incident. The options are as follows. The best option is listed first and then the second best and so on. This should only be taken as best practice advice and schools may need to undertake some business risk analysis to determine which is the best option for an individual school.

Option One Use of an off-site, central back up service

This involves a back up being taken remotely over a secure network (usually overnight) and stored in encrypted format in premises other than the school which have the appropriate security. EIS offers this service to schools for a fee.

Option Two Reciprocal Arrangement with another school

Schools may choose to make a reciprocal arrangement with another school to store the backups on their behalf. This would mean that each school would have to buy a data safe and travel to the school at the end of the day to lodge the back up.

This would have to be properly resourced in allowing time for a member of staff to leave the school premises before the official end of the day so that the exchange can be completed by the relevant members of staff. The same processes would need to be followed in terms of the management of keys and the locking of the box in the presence of a witness as laid out in option 3 below.

Option Three Storage in a data safe in another part of the school premises

On the larger, secondary school premises, or schools where there is joint ownership of the site, it may be appropriate to store the back up in a data safe which is stored in another part of the premises. These premises must be also be physically secure.

The back up must be placed in the safe in the presence of two people and the keys should either be stored in a locked key box, elsewhere on the site or allocated to another member of staff to take home with them.

Option Four Member of staff takes backup home

It must be stressed that this option should only be used if there are no other alternatives available.

This option should only be undertaken after a risk assessment has been completed and members of staff have been made aware of their responsibilities under the data protection legislation. If a breach of the legislation occurs at any time whilst the data is in the possession of an individual, that individual is personally liable.

There need to be some discussions with the Local Education Authority to see, if this option was the only option, whether the LEA could assume the liability provided the individual members of staff concerned were following the appropriate policies and procedures.

The backup would need to be sealed in a locked box (possibly a small data safe) in the presence of another person. The keys to the box would then be allocated to other members of staff to take home. The locked box must be stored out of plain sight whilst it is in an individual's home.

2. Major Environmental Incident

Fire and flood are two major threats to schools. These threats pose a greater risk to paper records than to electronic records (provided that the school has a robust backup procedure). In the event of a flood most if not all records can be salvaged. Fire, however, can be much more destructive of records and although fire damaged material can be salvaged it can be much harder.

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. Water damage is always much less severe if the water has first had to get into a receptacle. Metal filing cabinets have, in the past, proved a good first level barrier against fire (provided the heat does not force the drawers open).

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.

Individual schools need to undertake business risk analysis to identify which records are vital to school management and these records should be stored in a receptacle. Reference material, or material which could be easily replaced (phone books, supplies catalogues etc) can be stored on open shelves or desks.

For any further advice about business continuity issues in the record keeping context please contact Elizabeth Barber on elizabeth.barber@kent.gov.uk.

Information Audits

1. What is an information audit?

An information audit is the 21st century descendant of the records survey. However, an information audit can encompass much more than just “paper” records to include electronic documents, hybrid files² and “knowledge”. The information audit is designed to help organisations complete an information asset register (the 21st century descendant of filing classifications and disposal guidelines). The terminology grows out of the new concept of “knowledge management” which is gaining momentum; this concept involves the capture of knowledge in whatever form it is held (including encouraging people to record the information they have in their minds!)

It is now generally accepted that information is an organisation’s greatest asset (along with the people who use it) and that it should be managed in the same way as the organisation’s more tangible assets.

2. What are the benefits of the information audit?

The information audit is designed to allow organisations to discover the information they are creating and therefore store and to manage the information to get the most effective business use from it. For a local school the concept is much more concerned with accessibility of information. The information audit allows the local school to identify the personal information it creates and stores to allow correct management under the Data Protection Act 1998, and all the information it creates and uses to make the decisions which affect people’s daily lives which will become subject to the Freedom of Information Act 2000.

In other words an information audit collects the information necessary to formulate and implement an efficient records management programme (just like a records survey but more wide-ranging).

3. How to go about an information audit. [see also the flow chart]

The information audit works on a slightly different concept to the records survey. A records survey involved surveying records which have already been created and then fitting them into a scheme. The information audit works on the premise that all information is created for a purpose (*business need*) and the information created and stored is to support that business need. It works from the idea that everyone is far too busy to create information just for the fun of it.

The information audit works through a work-flow process [see the flow chart] identifying which information is created at which point in the process, what it is used for, how long it is needed and whether or not it should be captured as part of the “vital” record of the school (i.e. whether it is a working document or a final policy or report).

Once this process has been completed the information audit should contain a list of business needs, the kind of information created to meet that business need, in what format it is stored and how long it needs to be kept.

² Hybrid files are files which contain both paper and electronic information.

For example:

Bursar		
Business Function: Payment of Invoices		
Record	Format	Needed until
Invoice	Paper	6 years for audit
Payment authorisation	Electronic	Until payment is made
Payment made	Electronic	6 years for audit
Acknowledgement	Paper	6 years for audit

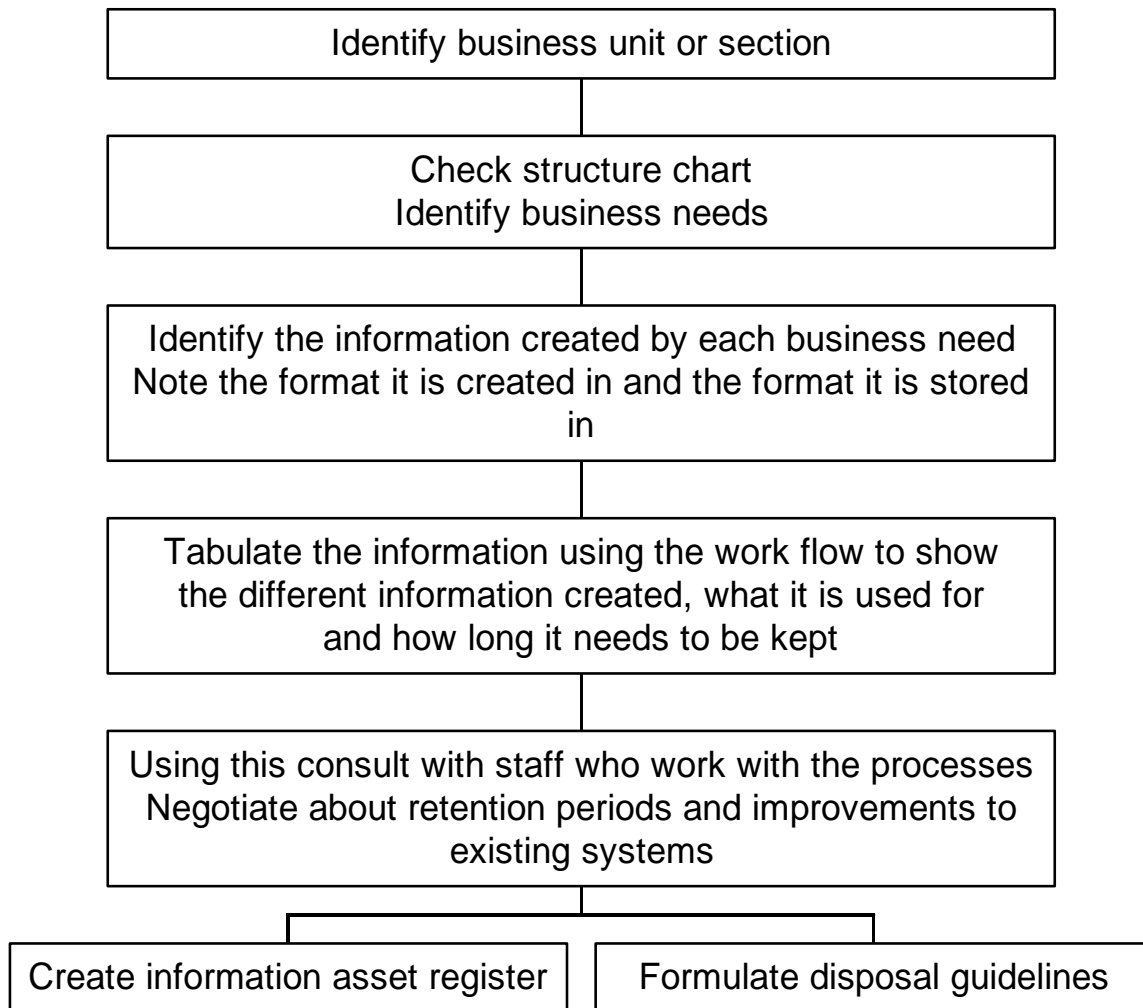
Once the information audit can be formulated like this then the person completing the audit needs to consult with the staff actually involved in the processes to ensure that this is an accurate reflection of what happens. At this point some negotiation may need to take place if there are any anomalies. The purpose of the information audit is to identify where processes can be improved, not merely to document what happens at present.

Once the information audit is felt to be accurate then the information can be tabulated into an information asset register if it is appropriate. This enables all members of staff to see what information is created, by which business process and how it should be managed. This helps with business continuity in the case of an emergency as members of staff are encouraged to consider what information they would need to carry on with their work.

The flow chart on the following page identifies each of the different stages of the process. To make it easier to determine the work flow, get the person who does the job to jot down all the stages in the process for you and where appropriate the records they create. You will be surprised at how straightforward this can be. If the person doing the job cannot identify the steps then there is probably something wrong with the process itself which needs to be looked at, or alternatively the person concerned needs to be shown how to understand why they are doing what they are doing.

For further information on carrying out information audits please contact Elizabeth Barber on elizabeth.barber@kent.gov.uk.

Information Audit



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. These guidelines are based on the assumption that the pupil record is a principal record and that all information relating to the pupil will be found in the file (although it may spread across more than one file cover).

It has become clear over a series of information audits that there is no real consistency of practice in the way in which pupil records are managed. These are intended to be guidelines to assist schools about how pupil records should be managed and what kind of information should be included in the file. It is hoped that the guidelines will develop further following suggestions and comments from those members of staff in schools who have to deal with these records.

These are only guidelines and have no legal status, if you are in doubt about whether a piece of information should be included on the file please contact Michelle Hunt on michelle.hunt@kent.gov.uk for advice.

1. File covers for pupil records

It is strongly recommended that schools use a consistent file cover for the pupil record. This assists the secondary school to ensure consistency of practice when receiving records from a number of different primary schools. In one secondary school there were at least three different kinds of file cover transferred for that year's intake. This led to the secondary school holding different levels of information for pupils which had come from different primary schools.

The pre-printed file covers issued by Kent County Supplies are a good example of best practice and should be used where possible. The use of standard document wallets should be avoided as it is very difficult to ensure that all the information required by the school is recorded consistently.

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. If the pre-printed file covers are not being used then the following information should appear on the front of 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

There has been some discussion about whether or not the pupil’s UPN should be recorded on the front of the file with the other information. It is perfectly acceptable to include the UPN on the front of the file as the computer system is password protected.

It is essential that as these files contain all this personal information that they will be managed against the [information security guidelines](#) also contained in the toolkit.

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)
- Fair processing notice [if these are issued annually only the most recent need be on the file]
- Parental permission for photographs to be taken (or not)
- Kent Years Record
- Annual Written Report to Parents
- National Curriculum and R.E. Agreed Syllabus Record Sheets
- 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

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 file in the event of a major incident)

3c. Transferring the pupil record to the secondary school

The pupil record should not be weeded before transfer to the secondary school unless any of the items mentioned above have been placed on the file. 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. Secondary School records

4a. Items which should be included on the pupil record

- Admission form (application form)
- Fair processing notice [if these are issued annually only the most recent need be on the file]
- Parental permission for photographs to be taken (or not)
- Kent Years Record
- Annual Written Report to Parents
- National Curriculum and R.E. Agreed Syllabus Record Sheets
- 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

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 once the pupil leaves the 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 file in the event of a major incident)

5. 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.

6. Safe destruction of the pupil record

The pupil record should be disposed of in accordance with the [safe disposal of records](#) guidelines.

7. 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 Michelle Hunt, michelle.hunt@kent.gov.uk for further advice.

If you have any comments about these guidelines or suggestions about how they can be further developed please contact Elizabeth Barber on elizabeth.barber@kent.gov.uk.

1. The purpose of the retention schedule

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 Data Protection Act 1998 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.

2. 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 Data Protection Act 1998 and the Freedom of Information Act 2000. Provided members of staff are managing record series using the retention schedule they can not be found guilty of unauthorised tampering with files once a freedom of information request or a data subject access requests have been made.

Members of staff can be confident about shredding information at the appropriate time.

Information which is subject to Freedom of Information and Data Protection legislation will be available when required.

The school is not maintaining and storing information unnecessarily.

3. Maintaining and amending the retention schedule

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

4. Useful Contacts

If you have a query about a retention period relating to a record series on the retention schedule or a query about the retention period for a record series which is not on the retention schedule then contact the Records Manager, Elizabeth Barber (01622-696581).

If you have a query about sending semi-current records to the Modern Records Centre then please contact the Assistant Records Manager, Jackie Davidson (01622-605237).

To arrange transfer of records to the Centre for Kentish Studies or the other Archive Centres mentioned above please contact the manager of the Centre for Kentish Studies (01622-694363)

Safe disposal of records which have reached the end of their administrative life

1 Safe destruction of records

Where records have been identified for destruction they should be disposed of in an appropriate way. All records containing personal information, or sensitive policy information should be shredded before disposal using a cross cut shredder. 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 the dustbin 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.

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
- The name of the authorising officer

This could be kept in an Excel spreadsheet or other database format.

2 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 Centre for Kentish Studies or Canterbury Cathedral Archives or the East Kent Archives Centre. Please contact the Manager of the Centre for Kentish Studies in the first instance unless you have already transferred records from your school in which case you should contact the Archives Centre you have contacted before. You may wish to explore the possibility of obtaining facsimile copies of the records for use in the school with the teams at the Archives Centres. The manager of the Centre for Kentish Studies is Julie Gregson and she can be reached on julie.gregson@kent.gov.uk.

If you would like to retain archive records in a special archive room on the school premises please contact the teams at the Archive Centres for advice.

3 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.

For further advice on safe disposal of records or you are considering transfer of data to other media please contact either Elizabeth Barber on elizabeth.barber@kent.gov.uk or Michelle Hunt on michelle.hunt@kent.gov.uk

School Closures and Record Keeping

When a school closes there will be records which will need to be stored until they work out their statutory retention periods. A full list of records can be found in the [retention guidelines](#) but some examples might include:

- Pupil records (DOB of pupil + 25 years)
- Accident reporting records (DOB of pupil + 25 years or date of incident + 7 years)
- Financial records (Current year + 6 years)
- Records relating to the employment of staff (Termination + 7 years)

It is the responsibility of the Local Education Authority to manage these records until they have reached the end of their administrative life and to arrange for their disposal when appropriate.

There may be a number of different reasons why a school has closed and this may affect where the records need to be stored.

- If the school has been closed and the site is being sold or reallocated to other use then the LEA should take responsibility for the records from the date the school closes.
- If two schools have merged onto one site and then function as one school, it is sensible to retain all the records relating to the two schools on the one site.
- If a secondary school closes and subsequently becomes an Academy, the records relating to the current pupil intake will be transferred to the Academy, but all other records become the responsibility of the LEA.

Sorting out records, when a building has to be vacated, is time consuming especially if records management has not been a priority in the past. Sufficient time to ensure that the records have been properly sorted, listed and boxed before transfer to the LEA must be allowed as part of the project timescales for the school closure. Proper resources must be allocated to this to ensure that the job can be completed before the school closes. It is much more difficult to sort records which have been boxed haphazardly in a hurry in the few days before the school closes.

It is important to bear in mind that when a school closes the staff teams may well feel a real sense of bereavement and this will affect the way in which they view the work which has to be done before the school closes. Sorting out records is usually low on the priority list, but nonetheless needs to be tackled. Managers will need to consider this when allocating the different elements of the task.

It is suggested that a project to sort out records could be managed in the following steps:

1. As soon as notification is received that the school is to be closed, a thorough review of all the records on the premises needs to take place. Agreement needs to be reached with the LEA about where the records which need to be stored until they can be disposed of will be sent and who in the LEA will be taking responsibility for them.
2. At this stage, if it has been decided to transfer records to the Modern Records Centre at Kings Hill, it is useful to make initial contact with the team at Kings Hill, contact either Jackie Davidson or Paul Baker on 01622-605237. This is a good opportunity to find out how the system works, order boxes and look at the allocation of MRC code numbers.
3. The next step is to identify all the records which can be safely disposed of using the retention guidelines. If you are unsure about what records can be safely disposed of contact Elizabeth Barber on elizabeth.barber@kent.gov.uk.
4. This should leave you with a list of the records which need to be transferred to the LEA. If it has been decided to send records to the MRC then e-mail a list of the record series (e.g.

pupil files, accident reports etc) to Jackie at the MRC and she will allocate MRC reference numbers for you to use.

5. The records need to be boxed up and listed in accordance with MRC procedures and sent to the MRC at Kings Hill.

If records need to be recalled to answer enquiries, this will be done by the LEA.

If you need further advice or assistance about how to manage records for a closed school please contact Elizabeth Barber on elizabeth.barber@kent.gov.uk or Michelle Hunt on michelle.hunt@kent.gov.uk.