EARDISLEY CE PRIMARY SCHOOL

Records Management Policy

Signed .....
Chair of Governors

Date of policy October 2014

EARDISLEY CE PRIMARY SCHOOL

Records Management Policy

This policy is taken from the Information and Records Management Society and the original document should be consulted as to full content and appendices etc.

The School recognises that by efficiently managing its records, it will be able to comply with its legal and regulatory obligations and to contribute to the effective overall management of the institution. Records provide evidence for protecting the legal rights and interests of the school, and provide evidence for demonstrating performance and accountability. This document provides the policy framework through which this effective management can be achieved and audited. 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 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 or received, and then stored, in hard copy or electronically.
1.3 A small percentage of the school's records may be selected for permanent preservation as part of the institution's archives and for historical research. This should be done in liaison with the local county archives centre.

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 about good records management practice 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
• Data Protection Policy
• and with other legislation or regulations (including audit, equal opportunities and ethics) affecting the school

Pupil Records

These guidelines are intended to help provide consistency of practice in the way in which pupil records are managed. These will 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 the most contact with pupil 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 the Local Authority.

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 to every school they attend 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).

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. If, for example, primary schools have many different file covers for their files, the secondary school that the pupil files were transferred to would then be holding different levels of information for pupils which had come from different primary schools.

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. 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.

2. Recording information

A pupil or their nominated representative have the legal right to see their file at any point during their education and even until the record is destroyed (when the pupil is 25 years of age or 35 years from date of closure for pupils with special educational needs). This is their right of subject access under the Data Protection Act 1998. It is important to remember that all information should be accurately recorded, objective in nature and expressed in a professional manner.

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

• Surname
• Forename
• DOB
• Special Educational Needs Yes/No [This is to enable the files of children with special educational needs to be easily identified for longer retention]

The file cover should also contain a note of the date when the file was opened and the date when the file is closed if it is felt to be appropriate.

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

• The name of the pupil's doctor
• Emergency contact details
• Gender
• Preferred name
• Position in family
• Ethnic origin [although this is "sensitive" data under the Data Protection Act 1998, the Department for Education 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]
• Any allergies or other medical conditions that it is important to be aware of [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 (and any additional relevant carers and their relationship to the child)
• Name of the school, admission number and the date of admission and the date of leaving.
• 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 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)
• 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 clearly marked as such).
• 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 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 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 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 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.

• 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

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 the Local Education Authority for further advice.

8. 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

1. 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 [1]
• Knowledge

The information audit is designed to help organisations complete an information asset register [2]. 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.
[1] Hybrid -les are -les which contain both paper and electronic information.
[2] The information audit is designed to help create fileplans, file classification schemes, retention/disposal schedule, identify vital records and the assigning of protective marking

2. What are the benefits of the information audit?
The information audit 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 Data Protection Act (DPA) 1998. NB. Under the DPA all schools, whether LA, Academy or independent 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. NB. Academies also fall under FOI (introduced in paragraph 10 of Schedule 2 of the Academies Act 2010) and should use the model publication scheme for schools.In other words an information audit collects the information necessary to formulate and implement an efficient records management programme and to ensure compliance with legislation.

3. How to go about an information audit

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.
The information audit works through a workflow process [see flow chart below] identifying which information is created at which point in the process, what it is used for, how long it is needed, 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) and whether it needs to be protectively marked.

The information audit can be conducted in a number of ways:

• Interviewing key staff from the key areas to identify the information and information flows etc.
• Sending out questionnaires to key staff to identify the information and information flows etc., although NB. These may be less likely to be returned as staff are busy and see a questionnaire as low priority
• A mixture of the above

Information Audit Flowchart

Create information asset register Formulate disposal guidelines
Identify the information created by each business need
Note the format it is created in and the format it is stored in
Check structure chart
Identify business needs
Identify business unit or section
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

Whichever option you chose it is important that you speak with senior management in order to get their buy-in and understanding of what it is and why you're doing it. Even if you decide to send out questionnaires it is important that you let staff know what it is you're doing and why. After all, they work with the information so they are best placed to identify it and any requirements. It also helps senior management and staff to start to understand their information responsibilities and should help ensure questionnaires are completed and returned on time.

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, the format in which it is stored, how long it needs to be kept, vital records status and any protective marking. Where local copies have been recorded by the information audit it might also be useful to stipulate who is responsible for retaining the master document/record (eg. local copies of minutes of a meeting may be kept by individual members of the school senior management team on a temporary basis but the Head will usually be responsible, as Chair of that meeting for the master set of minutes). For example: (Specimen only)

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, where it should be followed 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 results of the information audit should be presented to senior managers for comments and final approval. This will provide the audit with senior endorsement.

Finally, any information audit is only a snapshot in time and is only as good as the information which is provided by those taking part. Therefore in order for information systems to be kept up-to-date, including capturing information created by new and developing technologies, formats and to take account of new functions, and legislation the audit results should be regularly reviewed and updated.

Good Practice for Managing E-mail

1. Introduction

These guidelines are intended to assist school staff to manage their e-mail in the most effective way, and must be used in conjunction with your school's policies on the use of ICT.

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

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

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

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

E-mail is disclosable under the access to information regimes
All school e-mail is disclosable under Freedom of Information and Data Protection legislation. Be aware that anything you write in an email could potentially be made public.

E-mail is not necessarily deleted immediately
E-mails can remain in a system for a period of time after you have deleted them. You must remember that although you may have deleted your copy of the e-mail, the recipients may not and therefore there will still be copies in existence. These copies could be disclosable under the Freedom of Information Act 2000 or under the Data Protection Act 1998.

E-mail can form a contractual obligation
Agreements entered into by e-mail do form a contract. You need to be aware of this if you enter into an agreement with anyone, especially external contractors.

Individual members of staff should not enter into agreements either with other members of staff internally or with external contractors unless they are authorised to do so.

E-mail systems are commonly used to store information which should be stored somewhere else
All attachments in e-mail should be saved into any appropriate electronic filing system or printed out and placed on paper files.

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

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

3 Creating and sending e-mail

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

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

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

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

Ensure that the e-mail is clearly written
• Do not use text language or informal language in school e-mails.
• Always sign off with a name (and contact details).
• Make sure that you use plain English and ensure that you have made it clear how you need the recipient to respond. Never write a whole e-mail in capital letters.
• Always spell check an e-mail before you send it. Do not use the urgent flag unless it is absolutely necessary, recipients will not respond to the urgent flag if they perceive that you use it routinely.
• If possible, try to stick to one subject for the content of each e-mail, as it will be easier to categorise it later if you need to keep the e-mail.

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

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

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

4. Managing received e-mails

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

a. Manage interruptions
Incoming e-mail can be an irritating distraction. The following tips can help manage the interruptions.
• Turn off any alert that informs you e-mail has been received
• Plan times to check e-mail into the day (using an out of office message to tell senders when you will be looking at your e-mail can assist with this).

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

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

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

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

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

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

E-mail text and attachments
Where the text of the e-mail adds to the context or value of the attached documents it may be necessary to keep the whole e-mail. The best way to do this and retain information which makes up the audit trail, is to save the e-mail in .msg format. This can be done either by clicking and dragging the e-mail into the appropriate folder in an application such as MS Outlook, or by using the "save as" function to save the e-mail in an electronic filing system.
If the e-mail needs to be re-sent it will automatically open into MS Outlook. Where appropriate the e-mail and the attachments can be printed out to be stored on a paper file, however, a printout does not capture all the audit information which storing the e-mail in .msg format will.

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

the e-mail can be saved in .html or .txt format. This will save all the text in the e-mail and a limited amount of the audit information. The e-mail can not be re-sent if it is saved in this format.

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

How long to keep e-mails?
E-mail is primarily a communications tool, and e-mail applications are not designed for keeping e-mail as a record in a storage area meeting records management storage standards.
E-mail that needs to be kept should be identified by content; for example, does it form part of a pupil record? Is it part of a contract?
The retention for keeping these e-mails will then correspond with the classes of records according to content in the retention schedule for schools found elsewhere in the Records Management Tool Kit for Schools. These e-mails may need to be saved into any appropriate electronic -ling system or printed out and placed on paper files.

Information Security and Business Continuity

Information Security and Business Continuity are both important activities in ensuring good information management and are vital for compliance with the Data Protection Act 1998.

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)

1. Digital Information

In order to mitigate against the loss of electronic information a school needs to:
a. 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 back up being taken remotely over a secure network (usually overnight) and stored in encrypted format in premises other than the school.

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

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

b. Control the way data is stored within the school

Personal information must not be stored on the hard drive of any laptop or PC unless the device is running encryption software. Staff should be advised not to hold personal information about students or other staff on mobile storage devices including but not

limited to memory sticks, phones, iPads, portable hard drives or even on CD.

c. 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.

d. Manage the location of server equipment

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

e. Ensure that business continuity plans are tested

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

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

2. Hard Copy Information and Records

Records which are not stored on the school's servers are at greater risk of damage by -re and ood as well as risk of loss and of unauthorised access.

a. Fire and flood

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

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

b. Unauthorised access, theft or loss
Staff should be encouraged not to take personal data on staff or students out of the school, and where these records are held within the school they should be in lockable cabinets. You might need to 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 you should always log the location of the file and the borrower, creating an audit trail.

For the best ways of disposing of sensitive, personal information see Safe Disposal.

c. 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 have been identified to a cupboard or drawer (lockable where appropriate). It does not mean that the whole desk has to be cleared.

3. 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.
4. 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.

5. 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.
a. 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 appointed a named member of staff to liaise with the Information Commissioner's office if an information security breach needs to be reported.

b. Fire/Flood Incident
You should create a team of people who are trained to deal with a fire/flood incident. This will include the provision of an equipment box and the appropriate protective clothing. The team and equipment should be reviewed on a regular basis.

Safe disposal of records which have reached the end of their administrative life
NB: Please be aware that this guidance applies to all types of record, whether they are in paper or electronic form.

1. Disposal of records that have reached their minimum retention schedule the Data Protection Act 1998 stipulates that records should be kept for no longer than necessary.
In each organisation, local records managers must ensure that records that are no longer required for business use are reviewed as soon as practicable under the criteria set out so that ill-considered destruction is avoided.

The 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 at the end of this document.

Whatever decisions are made they need to be documented as part of a consistent and consistently applied records management policy within the organisation.

2. 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.

a. 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.
b. 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.

3. 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 Archives or the local records office. The school should contact the local record officce if there is a requirement to permanently archive the records, and the records will continue to be managed via the DPA 1998 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.

4. Transfer of information to other media

Where lengthy retention periods have been allocated to records, members of staff may wish to consider converting paper records to other media such as microform or digital media. The lifespan of the media and the ability to migrate data where necessary should always be considered.

Consideration should also be given to the legal admissibility of records that have been converted from paper to electronic media. It is essential to have procedures in place so that conversion is done in a standard way. This means that 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.