January 2015

Management of Information and File Retention Policy & Practice 2015-16

Whole School

Contains relevant information on the protocols around dissemination of information and document retention.

STANLEY SCHOOL WIRRAL

AUTISM ACCREDITATION

MANAGEMENT OF INFORMATION AND RECORDS POLICY

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

- Scope
- Responsibilities
- Relationships with existing policies

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

Records are defined as all those documents, which facilitate the business, carried out by Stanley 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.

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

Responsibilities
Stanley 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 Headteacher.

The person responsible for records management in Stanley 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 in a timely manner.

Individual staff and employees must ensure that records for which they are responsible are accurate, and are maintained and disposed of in accordance with Stanley School's records management guidelines.

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 Stanley School.

Records Management Guidelines

Finding out what records already exist and how they are being managed
The freedom of information legislation is completely retrospective so when a freedom of information request is received Stanley School will need to be able locate all the information on that subject. Therefore, it is important to ascertain what records exist currently and whether these records are still in operational use or whether they can be safely disposed of.

The best way to do this is by undertaking an information audit of the whole school if there is enough time available or of individual departments if resources are limited. The process is called an information audit rather than a records audit because it aims to cover all the information, which is created regardless of the format in which it is kept. This includes microfilm, electronic media and hybrid systems (i.e. systems which consist of electronic and paper records) as well as systems which are held entirely in paper format.

The information audit is based around all the different functions of the organisation. It works from the basic assumption that a business process creates information for a specific purpose. The retention schedule, which has been already created, could be used as a basis for the process to see which records Stanley School is actually creating and maintaining.

For the purposes of the Freedom of Information Act the audit also identifies which information is already being made public and which information could be made public as part of the overall publication scheme.

Once the information audit has been completed Stanley School will be aware of what information is routinely created and maintained and where it is located in preparation for answering freedom of information requests. There will also be the opportunity to identify records, which should have been safely disposed of in the past. Stanley School may wish

to order a skip (for the disposal of non-confidential records) and confidential waste bins (for the disposal of confidential records) and clears out the records as one project. Stanley School will also need to make arrangements to transfer any records, which are identified as being of permanent historical value to the Archives Service (see list of contacts).

Stanley School can also use this process to identify whether some of the records, which Stanley School stores in a paper format, could be created and managed electronically.

For more details about how to conduct information audit see Appendix A.

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 Stanley 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 that it is not necessary to manage this information against the same rigorous standards applied to manual systems.

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 law[1]. It can be extremely difficult to facilitate access to information under the freedom of information legislation using hybrid systems unless strict cLocal Authoritiessification 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.

Although the process outlined below can be seen to be time consuming, the end product will be a system which is compliant with the freedom of information and data protection legislation and will therefore facilitate the management of freedom of information requests and data protection subject access requests.

Creating a new information management system
[For more detailed information see Appendix B]

Maintenance of record keeping systems

It is important that filing information is properly resourced and is carried out on a regular basis. The information audit process may identify information, which no longer needs to be filed. 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, eLocal Authoritiestic bands, sticky notes and other accessories, which can damage the file, when the file is weeded. Where important information is contained on the sticky notes it should be photocopied and added to the file. Where possible a note should be made of the author's name, position and date if this is known. In the same way 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 opening 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 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 sticky tape to “mend” papers and not to use correction fluid 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 Local Authoritiest 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 Stanley School or in another appropriate place until it has reached the end of the retention period.

Information security is very important especially when dealing with personal information or sensitive policy information. There are a number of basic rules:

- All personal information should be kept in lockable filing cabinets which are kept locked when the room is unattended.
- 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.
- Files containing personal or sensitive information should not be left out on desks over night.
- Where possible sensitive personal information should not be sent by e-mail.
- If files need to be taken off the premises they should be secured in the boot of a car or in a lockable container.

Business continuity is also an important part of the information security process. If a major incident should occur (fire and flooding being the most likely), Stanley School needs to have ascertained what information is needed to carry on the business of Stanley School. This information should be entered onto a salvage plan so that in the aftermath of a major incident this information can be salvaged as a matter of urgency.

All computer information should be backed up regularly and the back up should be stored off the site. There is no point in completing a back up if that back up is then damaged in the same incident as your system.

Where possible all paper information should be stored in a filing cabinet or cupboard. Information, which is left unprotected on desks and shelves, is almost certain to be irretrievably damaged in the case of fire or flood.

There is a common myth that e-mail should be managed differently from any other kind of information. E-mail is just the vehicle for transporting information in the same way that an envelope carries a letter, a fax machine prints a fax and so on. Information contained in e-mail should be filed into the appropriate electronic or manual filing system once it has been dealt with. [see Appendix C for further information about dealing with e-mail]

The safe disposal of information using the retention schedule

The retention periods laid down in the retention schedule constitutes “normal processing” and providing files are being managed against the retention schedule members of staff cannot be prosecuted for tampering with files.

Stanley School needs to have a protocol in place to weed out the files on a regular basis. This might be on an annual basis, for example in the first week in January or alternatively the first week in April, or at the end of August in preparation for a new term. If the information has been retained it will be disclosable under freedom of information so it is important that the process is undertaken routinely rather than when the storage area is full, or no one can see the floor any longer!

Where possible all personal information should be shredded before disposal for pulping. Other files can be bundled up and put in a skip or disposed of to the waste paper merchant. Loose papers should not be put in skips unless the skip has a lid. These papers have a habit of blowing down the street to be picked up by alert members of the public or journalists! Records Centre staff are happy to give advice about the safe disposal of records in this way.

If the process is undertaken on a routine basis, it makes it more straightforward to order a skip, secure data disposal bins or a shredder. The Archives Service can then be alerted that there may be a transfer of records to the Archives at that time.

Retention Schedule for Schools
This has been issued as a separate document.

Useful Contacts:

For enquiries about Archives please contact: **Jan Hughes 648 3171**

For enquiries about records management and retention periods please contact: **Jan Hughes 648 3171**

For information about freedom of information and information management please contact:

Steve Coulson 666 4321

For information relating to data protection and freedom of information relating to Education please contact:

John Bulmer 666 4337

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 files[2] and "knowledge". The information audit is designed to help organisations complete an information asset register (the 21st century descendant of filing cLocal Authoritiessifications 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.

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).

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 Stanley 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.

For example:

Bursar		
Business Function: Payment of Invoices		
Record	Format	Needed until
Invoice	Paper	6 years for audit

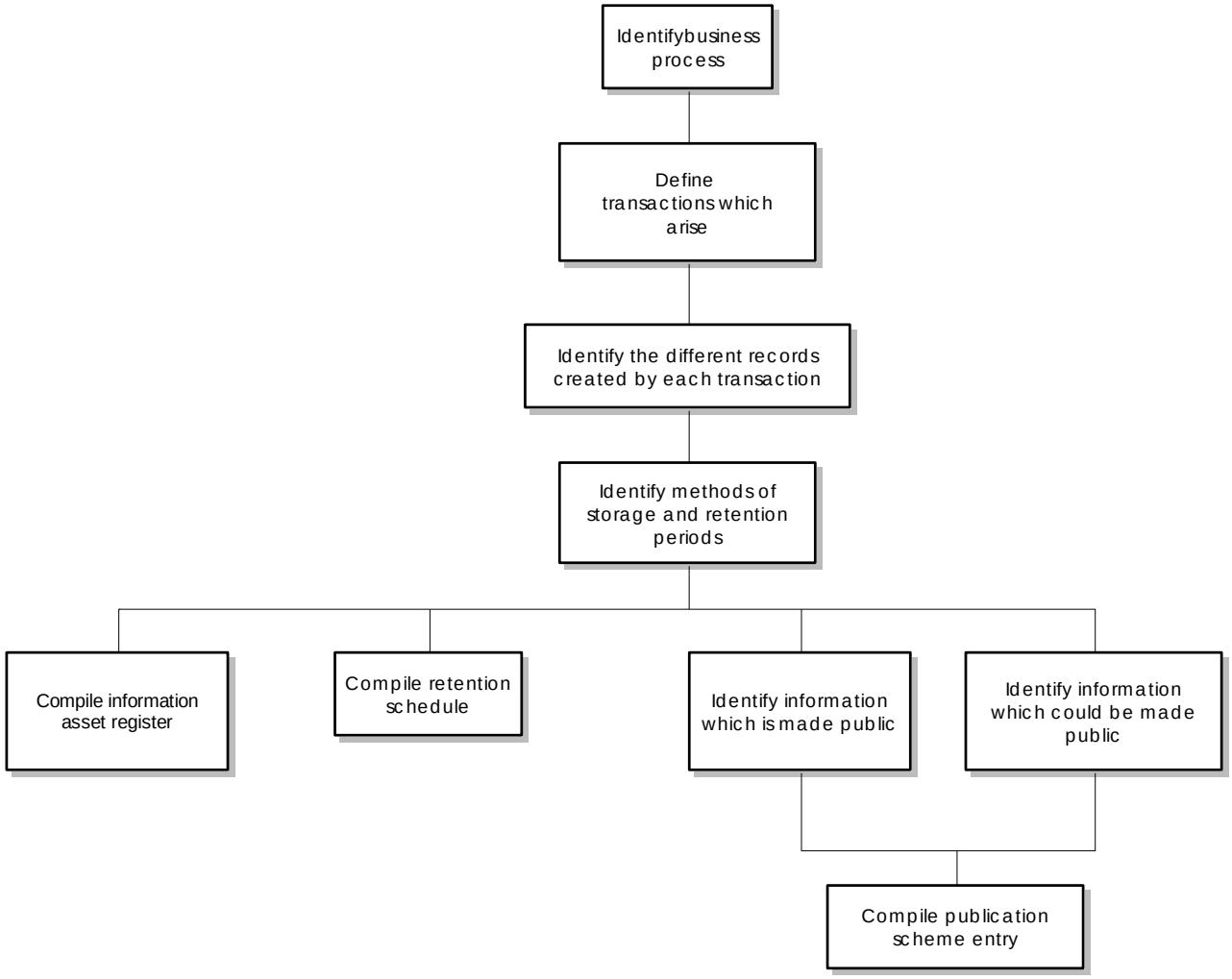
[2] Hybrid files are files that contain both paper and electronic information.

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 which business process creates what information, 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 workflow, 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.



Appendix B: Creation of an information management system

- 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 cLocal Authoritiessification scheme needs to be created. Since the demise of the central filing registries, effective file cLocal Authoritiessification schemes are not always created when new information management systems are introduced. Filing cLocal Authoritiessification 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 cLocal Authoritiessification 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 MS Windows 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).

  Alphanumeric systems, which connect with the business process, are generally easier for users to remember and use effectively.

- Once the cLocal Authoritiessification 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 Stanley 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 has been determined, an initial retention period needs to be allocated to them and the record series need to be added to Stanley 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 as other information received by members of staff.

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.

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 is 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 do not 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 auto reply in a number of different creative ways. Your message can state that:

- You are out the office and when you are back;
- 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.

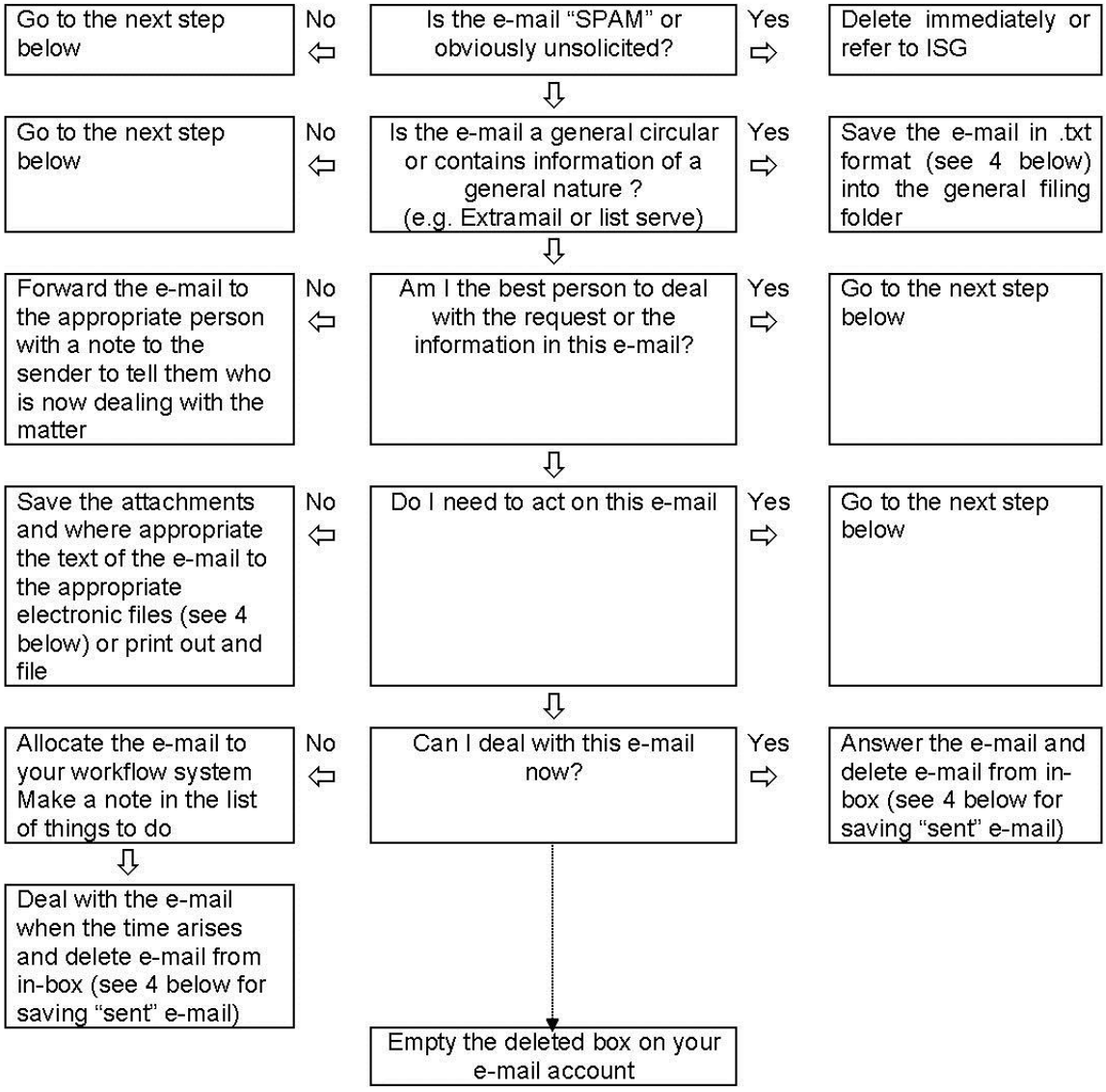
If you have to forward an e-mail to someone else to deal with, it is a good idea to send a reply to the sender to tell them you have referred it on and who to contact if they have a query. This will save you being hassled by the sender when the person who should be dealing with it has failed to reply!

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.


Is the e-mail "SPAM" or obviously unsolicited?
No
Go to the next step below
Yes
Delete immediately or refer to ISG
Is the e-mail a general circular or contains information of a general nature ? (e.g. Extramail or list serve)
No
Go to the next step below
Yes
Save the e-mail in .txt format (see 4 below) into the general filing folder
Am I the best person to deal with the request or the information in this e-mail?
No
Forward the e-mail to the appropriate person with a note to the sender to tell them who is now dealing with the matter
Yes
Go to the next step below
Do I need to act on this e-mail
No
Save the attachments and where appropriate the text of the e-mail to the appropriate electronic files (see 4 below) or print out and file
Yes
Go to the next step below
Can I deal with this e-mail now?
No
Allocate the e-mail to your workflow system Make a note in the list of things to do
Deal with the e-mail when the time arises and delete e-mail from in-box (see 4 below for saving "sent" e-mail)
Yes
Answer the e-mail and delete e-mail from in-box (see 4 below for saving "sent" e-mail)
Empty the deleted box on your e-mail account

Saving and storing e-mail

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).

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.

This may be an electronic system in an electronic system:

- Select the e-mail and find save as on the file menu
- Save the e-mail as a .txt file using the agreed file naming conventions
- Right click on the attachment icon and save as to the appropriate file using the agreed file naming conventions.

This may be a paper system:

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

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

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.

In order to do this you need to highlight all the sent e-mail in your sent e-mail box and then select the save as option on the file menu. You save the file as .txt – this saves all the e-mails with their headers into one file. You can then convert the file to MS Word if you wish. If you think you may need to guard the legal integrity of the data then it is a good idea to burn them to a CD or to investigate turning them into a .pdf file. Once you have completed this operation you can delete all the sent e-mails, not forgetting to empty the "delete" box.

DATA PROTECTION ACT LEGISLATION
(Updated: October 2010)

REQUIREMENTS WITH RESPECT TO "FAIR PROCESSING" UNDER THE DATA PROTECTION ACT AND THE PASSING OF INFORMATION TO CONNEXIONS

"Fair processing" under the Data Protection Act

Schools, Local Authorities (Local Authorities), the Department for Education and Skills (DfES), the Qualifications and Curriculum Authority (QCA), Ofsted, the Learning and Skills Council (LSC), Department of Health (DH) and Primary Care Trusts (PCTs) are all "data controllers" under the Data Protection Act 1998 in that they determine the purpose(s) for which "personal data" (i.e. data about living individuals from which they can be identified) is processed and the way in which that processing is done. This guidance deals specifically with personal data about pupils, although personal data may also be held on other groups such as teaching and non-teaching staff, and similar considerations with regard to "fair processing" will apply to them.

Data controllers have to provide "data subjects" (individuals who are the subject of personal data) with details of who they are, the purposes for which they process the personal data, and any other information that is necessary to make

the processing of the personal data fair, including any third parties to whom the data may be passed on. This is referred to as a "fair processing notice".

In respect of the Data Protection Act there is a presumption that a child of twelve years of age and over has sufficient maturity to exercise their rights under the Act, though in practice there will be exceptions to this. This is endorsed by guidance issued by the Information Commissioner.

The fair processing obligations on the data controller may appropriately be met by providing a fair processing notice to the parent (or the person with parental responsibility) where a child is younger than twelve, though the parent should be encouraged to share it with the child if the child has the maturity to understand it. However where the child is aged twelve or more, the fair processing notice should be provided both to the rights of the child and the parent's need to be aware of how their child's information is handled.

Further information about fair processing requirements, and guidance on the Data Protection Act generally, can be obtained fro the Information Commissioner's website (http://www.ico.l:lov.uk/eventual.aspx?id=34).

The suggested text of the fair processing notice is set out at the end of this guidance.

Local Authorities should work with schools to ensure that:

- Schools issue the fair processing notice to all current pupils of the age of 12 and over and to their parents and to the parents of all current pupils under the age of 12 as soon as possible, even if a fair processing notice has been previously issued to them; this is to ensure that all are informed of any additional data collection and any changes in the use of the data;

- This notice covers processing carried out by Local Authorities, DfES, QCA, Ofsted, the LSC, DH and PCTs as well as by Stanley School (rather than these organisations sending separate notices, which would be logistically very difficult and confusing for parents).

- Schools issue the same notice to new pupils and/or their parents as part of the enrolment process;

- Schools reissue the notice to pupils at age 16, to draw to their attention that the right under the Learning and Skills Act to opt out form the passing on of information over and above name and address of pupil and parent to those providing Connexions services, passes from the parent to the pupil at that age. It is suggested that the notice should be reissued to pupils at the beginning of the term in which they reach 16, and not on each individual pupil's birthday.

Schools are not issued with separate guidance about the issue of the fair processing notice and so Local Authorities should act promptly to ensure that schools receive the notice and substitute it for the previous notice.

Most of the fair processing notice relates to all schools, but there are two versions of the sections about pupils' rights under the Data Protection Act and passing information to Connexions – the first for schools which do not have pupils of secondary age, and the second for schools which do.

Before forwarding the text to schools Local Authorities will need to consider the adequacy of the paragraph describing the uses of personal data by the LA, and also insert contact details for the Authority's Data Protection Office.

As well as issuing the notice directly to parents or pupils, schools may also include this notice in other communications with parents (e.g. Stanley School prospectus, the governors' annual report, the individual pupil report, or the annual data checking sheet), and/or display the text on a school website or in a prominent location in Stanley School. These are not however requirements, nor are they a substitute for the arrangements indicated above.