Records Management In Schools

A Six Paper Series by Neil Maude of Arena Group Ltd

The Information and Records Management Society (IRMS) curates a regularly updated "Records Management Toolkit" written specifically to assist UK public sector schools in their compliance with the Freedom of Information Act 2000. In a series of articles, Arena's Neil Maude looks at the practical application of the principles described in version 4 of this toolkit. Neil's advice draws upon Arena's 20+ years of experience in the provision of document management solutions within and outside of the education sector.

NEIL MAUDE

Neil joined the Arena Group in 2006 and has almost 20 years of experience in the electronic document management industry, working with both private and public sector customers. Neil sits on Arena's board of directors and manages the delivery operations of Arena's EDM business. His team spend their time developing software, implementing solutions for customers and providing after-sales software support services, both in the UK and internationally.

Contact Neil Maude
Electronic Document Management
General Manager

T : 0844 863 8000
E : NeilM@arenagroup.net
🐦: @nmaude2006

Arena group

T: 0844 863 8000
E: info@arenagroup.net
W: www.arenagroup.net
🐦: @ArenaGroup

Records Management in Schools Part 1: **Developing a Records Management Policy**

Before we get into the detail of records management and the practical elements of implementing a policy, there is a fairly obvious first question to ask. Most schools have been around for a while – some for a very long while – and already have processes in place to manage documents in line with legislation and sector best practice. So is there really a need to change? We believe there are 3 compelling reasons for a school to take a good look at the way it manages records and information:

- **Legislation** – there's plenty of it and it's increasingly vigorous. Schools are subject to Freedom of Information and Data Protection rules, just like any other public organisation. In the event of a breach, the Information Commissioner's Office (ICO) can, and sometimes does, impose fines or require organisations to sign undertakings to improve processes. Clearly it is better to be proactive and prepared.

- **Retention requirements** - The amount of information being retained is ever growing, increasingly time-consuming and expensive to deal with. As well as cost, this might lead to problems with storage – especially for schools in a new building with limited space to store paper files. Academies may be required to retain even more records - those previously held by the LEA - creating another new problem.

- **Continued improvement** - There is an expectation of continual improvement in every organisation. Record keeping should be no exception.

With these points in mind, the IRMS Toolkit becomes a very useful framework within which to revise or refresh your procedures.

What is a record?

The IRMS defines a record as *"all those documents which facilitate the business carried out by the school and which are thereafter retained … to provide evidence of its transactions or activities. These records may be created or received, and then stored, in hard copy or electronically."*

Every item of data you create is a record – from formal typed documents to handwritten permission slips and every single e-mail. That's a pretty daunting list.

This definition pretty much means that every item of data you create is a record – from formal typed documents to handwritten permission slips and every single e-mail. That's a pretty daunting list. Clearly some records are more valuable than others and there are various pieces of legislation and guidance as to how long each record should be retained. All of which adds complexity.

Starting Point: Developing a formal Records Management Policy

The IRMS Toolkit recommends starting with a formal written records management policy or code of practice that sets out the scope, responsibilities and links to other existing policies.

This policy needs to be endorsed by senior management and readily available to staff at all levels. The document should provide a mandate for records and information management and a framework for supporting standards, procedures and guidelines.

The precise contents of the policy should, as a minimum:

- Set out a commitment to create, keep and manage records which document the principal activities of the school
- Outline the role of records management, identifying and making appropriate connections to related policies, such as those dealing with email, information security and data protection
- Delegate roles and responsibilities for creating and using records appropriately
- Indicate how compliance with the policy and the supporting standards, procedures and guidelines will be monitored
- Outline how the policy will be reviewed and updated. This should be done at regular intervals and following any significant changes that may affect records management.

The IRMS suggests that one senior representative for the school should take overall responsibility for implementing the policy.

The IRMS Toolkit includes a template which needs only the school name to be inserted and the document is then signed as a formal record of the school's commitment to its implementation.

This is a good starting point because it clearly demonstrates and allocates responsibility. With the legislative implications, it's hardly surprising that the IRMS suggests that one senior representative for the school (e.g. Head teacher) should take overall responsibility for implementing the policy. A second important point to note is that this person should also be responsible for providing guidance and promoting good practice. This is a little more contentious, as there is a time implication so it may be that this task is delegated and then audited.

Find the latest version of the IRMS Toolkit at ***www.irms.org.uk***

Records Management in Schools Part 2: **Conducting an Information Audit**

Information is generally accepted to be a key asset in any organisation and should be managed with the same care as more tangible assets such as money, buildings and classroom equipment. Effective information management is all about keeping information secure and getting it to the right people at the right time. The IRMS Toolkit rightly states that an information audit is a key step to achieving these aims.

What is an Information Audit?

Simply put, the information audit is a survey of the records being used and held by the organisation. It's a structured process of finding out what you have, where it is kept and how it is used. The IRMS toolkit suggests a step-by-step process which encompasses the same principles that Arena has used extensively in both the education and wider public/commercial sectors.

Step one: Secure a senior sponsor

The audit process requires a lot of in-depth access to information and discussions with key staff so it's important to have good senior backing. Make sure you also clearly explain the purpose behind the audit process to those involved, so everyone understands the aim of the exercise.

Step two: Identify key personnel

The information audit begins with the assumption that records are created for a particular purpose. Therefore, the ideal starting point is an organisational diagram or similar chart, showing the key functions. From this, we can identify the key staff to interview with regard to what information assets they manage. The IRMS suggests that the survey work could be via interview or questionnaires – from experience I would strongly recommend the face-to-face approach, as the quality and detail of feedback is invariably much better.

Step three: Map your document pathways

Once key people are identified, work with them to make a list of records being created. It often helps to think of the work being done as a chain of actions – often the document will go to other areas of the business and it is important to capture this journey.

> ***The audit process requires a lot of in-depth access to information and discussions with key staff so it's important to have good senior backing.***

Step four: Ask pertinent and insightful questions

The IRMS Toolkit contains an excellent checklist of questions to ask about each record type to cover areas such as key points of access, security and retention/disposal. The next features in this series will explore these points in more detail.

There are two additional key areas for consideration which can draw significant insight and additional benefit from the audit process, so it's well worth making an effort to include them in your agenda when you are speaking to your information curators:

- ***Room for improvement:*** The audit is an opportunity to identify potential process improvements. Although it will need to be handled sensitively, a certain amount of "and why do you do it that way?" analysis can be undertaken.
- ***Continuity planning:*** Another good question to ask is "what if you lost all of the information of this type – maybe in a fire – how would this affect you and what would you have to do about it?" This will help to determine the importance of records (operationally, if not legislatively) and give a head-start for disaster and risk-reduction planning.

It is difficult to see any organisation achieving a successful records management policy without a complete and regularly updated information audit.

Step five: Review, update, repeat …

Finally, the audit should be considered a snapshot in time. Like any other audit, there should be a clear plan as to how the findings will be refreshed and kept current. Any process changes arising from the audit should also be subject to a 'plan-do-check-act' cycle of implementation and verification.

A complete and comprehensive information audit also puts the organisation in a state of readiness to update, or indeed create, a meaningful records management policy – covered in part one of this series.

The information audit is an important early step in the implementation of an electronic document and records management system (EDRMS). It is difficult to see any organisation achieving a successful records management policy without a complete and regularly updated information audit.

Records Management in Schools Part 3: **Information Access and Security**

The protection of information relating to children is clearly a key responsibility and it is an obligation that is shrouded in layers of legislation. It is tempting to think that locking away your information and restricting access is the best way forward but this can slow down and frustrate day-to-day work. Some information, such as medical records, must be both quickly available and restricted only to those who need to see it; so information access and security should be considered together and in balance.

Two particular pieces of legal guidance to be aware of

The Freedom of Information Act (FoIA) states that schools must respond to requests for information pertaining to individual pupils in a timely fashion. Failure to meet FoIA requests can and does lead to action by the Information Commissioner's Office (ICO). Planned changes to Special Education Needs (SEN) legislation are expected to deliver increased numbers of requests.

Compliance with BSi10008 enables you to destroy paper files, whilst ensuring that the electronic copies remain legally admissible. Schools are required to produce a full audit trail to prove the veracity of their documentation. They must also implement a mechanism to prove that documents have not been tampered with and employ a retention policy.

Practical steps towards compliance

Having developed a records management policy and conducted an information audit you are in a good position to decide how to implement access controls for your documents.

Compliance can be complex and problematic if you are working with scattered documents that are stored in several different ways. For example, you may have some paper child protection documents in a locked cabinet accessible only by your child protection officer. Other documents relating to the same pupil may be stored in your admin office or held in your SIMS database, computer files and applications (such as email inboxes) or digital storage devices. A sensible first step is to minimise variations in document formats and locations. A good electronic document and records management system (EDRMS) can assist this by bringing documents and storage systems together for access via one reference point.

Whether you are working with paper or digital files – or a mix of both, there are some important legal compliance questions to address. These are explained on the following pages and cover four key areas of storage, completeness, movement and confidentiality.

> ***Compliance with BSi10008 enables you to destroy paper files, whilst ensuring that the electronic copies remain legally admissible.***

Storage

*"Pupil records should be kept securely at all times. Paper records 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." – **IRMS Toolkit.***

***Question:** How do you store your records? How do you guarantee that they are never left unattended and/or seen by unauthorised people?*

- ***Paper:*** The IRMS suggests a clear desk policy involving the removal of physical records to locked storage facilities whilst they are not in use, whilst restricting access to offices where confidential files are being stored or worked on. It is likely that you will need to split records in order to store sensitive documents separately, for access only by authorised people.

- ***EDRMS:*** Allocate login details and access rights to individual users so that they can only access file types that they are authorised to see. For example, your child protection officer will be able to see sensitive records that a secretary working in your admin office will not be able to see. You can prevent sensitive documents from being shared, printed, deleted and/or over-written. Computer monitors can be set to switch to stand-by after a set period of inactivity, requiring the user to enter a password to re-activate the screen. This means documents left on-screen at unattended desks will be protected.

The way you log where physical files are placed, and your strategies for avoiding filing errors, are fundamental.

Completeness

*"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. This is their right of subject access under the Data Protection Act 1998." – **IRMS Toolkit.***

ICO judgements against schools falling foul of the FoIA have, to date, been largely for failure to comply with requests in a timely or complete fashion.

***Question:** If you were asked to provide a copy of every document you have ever stored on an individual pupil, how easily could you respond and could you be absolutely certain that you had a complete file with not a single document missing?*

- ***Paper:*** With the ICO list in mind, the location of information is paramount. Physical filing can be a problem in that files can only be in the hands of one person at any one time, are often not replaced and are at risk of being lost. Your storage and archiving system is critical. The way you log where physical files are placed and your strategies for avoiding filing errors are fundamental to ensuring that you can rapidly bring together comprehensive information.

- ***EDRMS:*** Search facilities provide immediate and comprehensive access to documents that can be accessed via the system. This simplifies preparation for audits and FoIA requests whilst reducing the risk of missing information – providing the EDRMS is a central document store.

Movement

"Staff should be encouraged not to take personal data on staff or students out of the school." – ***IRMS Toolkit.***

Question: *Does paperwork ever leave your premises? If so, how do you keep it secure?*

- ***Paper:*** The IRMS guidance here is to check paper files out from a central system and log details of the borrower to create an audit trail. This does require an element of trust as you cannot control what happens to documents once they leave your building. There is also a risk of human error when it comes to logging - and document theft or loss outside of school.

- ***EDRMS:*** Data that is held on your servers may be securely accessed remotely by authorised employees, negating any need to ever transfer data onto a portable device such as a laptop. This mitigates several risks that arise from allowing documents to leave your premises – including theft, damage and loss.

Confidentiality

"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." – ***IRMS Toolkit.***

Question: *How do you ensure that only authorised personnel can access confidential information? How do you monitor and evidence this? How quick and easy is the process?*

- ***Paper:*** Documents can only be held in one location, so ensure that only authorised people can access them using lockable storage. In addition, consider placing record sheets into sensitive files to log access information.

- ***EDRMS:*** In addition to the security functionality detailed above (logins and permissions), an EDRMS system has the benefits of an audit trail of user activity. This allows the adoption of much more of a trusted approach to security, as well as being a key component of ensuring that your electronic records remain legally admissible. Unlike files saved on disks or similar media, an EDRMS compliant with BS10008 allows you to use electronic documents as evidence. Clearly, you should only consider disposing of your paper records if your EDRMS holds legally admissible information.

Paper documents can only be held in one location, so ensure that only authorised people can access them using lockable storage.

Approaching access and security with a view to making information available quickly to those who need it is a great aid to both implementing the policies developed from your information audit and ensuring that you are well placed to cope with the demands of prevailing legislation.

Records Management in Schools Part 4: **Information Disposal**

Information stored by schools has a fairly fixed working life but relevant data may be required to be held for a considerable period after a particular student has left the school. This can be for all sorts of purposes, including confirmation of attainment and a whole host of legal matters. Obviously, this means that there is a considerable storage burden which is borne by the final school attended by a given student. This burden may persist for many years, in some cases until the former student has reached 30 years of age.

What the law says

Two key pieces of legislation come into play with regard to the long term retention of student files (and any other information generated by the school).

Firstly, there is the Data Protection Act (1998), one of the central principles of which is that: “Information shall not be kept longer than is necessary”

This is a clear call to dispose of information when it is no-longer required. Indeed, roughly half of the IRMS Toolkit is an extensive list of how long to keep records of a particular type.

The second relevant piece of legislation is the Freedom of Information Act (2000), which provisions for subject data access requests (SARs) by individuals who wish to see any and all personal information which may be held regarding them.

When considered alongside the longer term storage requirement, these pieces of legislation create a complex picture for information retention and disposal.

Typical problems surrounding Information Retention and Disposal

There are obvious issues of space if paper documents are simply stored long term in a file room. It is likely that at some point you will run out of space or – as in the case of many new-build schools – there may simply be no space (Arena’s Lisa Butterworth has written a separate piece on physical storage in BSF schools, which can be found on the Arena website).

Regardless of space, simply placing documents in deep storage has 3 key problems:

1. ***Finding a given record*** – in an increasingly cluttered store – is going to be a challenge that no-one wants to tackle. Certainly, this is unlikely to be done quickly and there may be some doubt about whether it could be done comprehensively in the event of a subject data access request (SAR).
2. ***By law, a school cannot retain documents beyond their set retention periods.*** Older files will need to be removed at some point – even if this is by whole years of filing at a time. A store full of paper represents a future archiving challenge and there are costs for bulk destruction services.
3. ***Storing documents in this way is not legally compliant with the Data Protection Act.*** A school adopting this approach will also be hard pressed to prove compliance with Freedom of Information requests.

It’s worth remembering that the same principles, problems and legislation apply to documents relating to pupils, staff, governors and the financial management of the school. Whilst points 1 and 2 may be something that a school could live with, accepting the associated costs, point 3 is a major compliance issue that cannot be ignored.

Options for managing paper

A potential solution could be to periodically remove and destroy paper documents from the archive which are no-longer required under retention laws. However, faced with potentially thousands of files containing millions of pages, this is likely to be massively time consuming.

For example, if it takes 5 minutes to retrieve a file and manually search through the contents for a particular type of document (a not unreasonable time for a 200+ page file) then repeating the process for a full year group of 500 students would take one person more than a week. This multiplies out for larger schools, manually archiving many years’ worth of files (remember - all kept until the former student is 25) and taking care to retain or remove file types with varying retention dates.

Safeguarding must be a consideration if you choose to manually archive paper files. Sensitive files, for example those pertaining to child protection, must be handled only by authorised employees. (Read more about this in issue 3 of this series).

Also, manual sorting of numerous files can be fraught with human errors, so frequent rest breaks are advisable in the interest of refreshing tired eyes.

An alternative solution

Space issues can be addressed by scanning paper files and storing them electronically. Provided you have a system that enables compliance with BSi10008 (a standard and code of practice which ensures the evidential weight of documents stored electronically), you can destroy the original paper documents.

A good electronic document and records management system (EDRMS) will apply retention rules to each part of a classification of documents stored in the system. Documents are stored against the appropriate classification (eg; attendance, admission, parental permission forms, SEN statements). The system can then apply rules to dispose of documents or present them for review on a set date – possibly with reference to pupil specific information, such as date of birth. This approach dramatically reduces the management time associated with retention and completely eliminates the issues associated with large physical paper archives.

Simple scanning of documents into folders on the school’s network, or other internal databases, does not provide adequate functionality to properly manage the retention and disposal of documents.

It’s important to note that simple scanning of documents into folders on the school’s network, or other internal databases, does not provide adequate functionality to properly manage the retention and disposal of documents. This approach is not compliant with BSi10008 and is often fraught with problems relating to document retrieval and network capacity, making a specialist EDRMS a much more practical solution.

Of course, success also depends on an appropriate records management policy being enforced within the school, routine information audits (as explained in my previous articles) and matching the outcome of these audits to the retention guidance provided in the IRMS Toolkit. If all of this works as it should, the school can confidently place documents into an electronic store and destroy the original paper documents.

In the eyes of the law, the headteacher maintains overall responsibility for the records and information held.

Things to consider

- ***Legal admissibility of electronic documents:*** Following the destruction of paper records it is important that a school can rely on electronic information if called upon to provide evidence for a legal case. Assurance on this matter is provided by an EDRMS that complies with the guidance in BSi10008, the code of practice for legal admissibility of documents stored electronically. This standard requires that the EDRMS has sufficient auditing to demonstrate the provenance of a given document, including who created the document and when.

- ***Freedom of Information Act (FoIA):*** In the event of a request under FoIA, it may be necessary to evidence that a full and complete response has been provided to a subject data access request (SAR). For this reason, the IRMS Toolkit states that the school should maintain a list of records which have been destroyed and how this was authorised. Thereby, the school can protect itself from any allegation of failing to provide the requested information. A good EDRMS will automate this.

- ***Hardware and backup media disposal:*** An EDRMS will be part of data backup processes, typically meaning that copies of the system will be stored on magnetic backup tapes. For complete compliance, it is necessary that these tapes are subject to a destruction plan; otherwise the school may be retaining information unlawfully.

Further, the school should consider disposal processes for obsolete computer equipment. The IRMS Toolkit suggests that hard drives should be “dismantled and sanded”, which is the ultimate way of ensuring that data cannot be recovered (in fact, Google crush and shred hard drives that are no-longer required). However, this does seem a little excessive and commercial software is available to over-write disks, ensuring that data cannot realistically be recovered from them, after which the disks can be recycled rather than sent to land-fill.

Evolution of the rules

One final point to note is that retention requirements are evolving. The IRMS toolkit was last updated in May 2012, but already we are seeing customers with emerging needs that post-date this document. This evolution is often stimulated by developments in technology and processes adopted by schools; for example, we recently worked with a school that needed a new document classification and retention rule for biometric data permission slips.

Whether you choose to work with paper or electronic files, it is essential to keep on top of the information retention and disposal issue as rules continue to change. A school is required to nominate someone to update its policies and processes in line with changing legislation. In the eyes of the law, the headteacher maintains overall responsibility for the records and information held. Installing an EDRMS gives you the support and expertise of an external provider, and a practical, automated means to manage the increasing burden.

Records Management in Schools Part 5: **Email Management**

E-mail has become the communication tool of choice for most office workers. It is quick and cheap, with the convenient benefit that the recipient of your message doesn't have to be available when you are. However, even though e-mail, like a letter or a memo, is just another way to pass on a message, somehow we treat it differently. For starters, e-mails tend to be written using less formal language and most people spend less time on the layout of an e-mail than they would if sending the same message in a letter. This doesn't change the fact that an e-mail is a formal record, just like any other piece of written communication – and therefore subject to the same obligations, duties of care, controls and legislation.

Although the IRMS toolkit has a separate section for e-mail management, in the same way that this series is discussing e-mails specifically, the same principles apply as for any other paper or electronic documentation. In particular, e-mails sent or received by a school are subject to the same Data Protection Act (1998) and Freedom of Information (2000) legislation as any other information held.

Where e-mail is different

Besides the less formal use of e-mail, there are some key points which set it apart from other documents and records.

- **An e-mail system comes with the innate ability to store material.**
  It's very easy to create folders, retain sent messages and so on. Without appropriate policies in place, e-mail can rapidly become an unofficial and unmanaged information repository.

- **Email volumes can be high and correspondence can involve large groups of people.**
  This can make management of email time-consuming, or even stress-inducing.

- **The speedy and informal nature of email can lead to unintended consequences.**
  There is far more potential for a recipient to misunderstand a quick e-mail note than would be the case with a carefully crafted letter or a phone call.

E-mail is a formal record, just like any other piece of written communication – and therefore subject to the same obligations, duties of care, controls and legislation.

The IRMS toolkit contains a number of techniques for addressing the second and third points above. These include appropriate communication standards, awareness that an e-mail is a communication like any other (and so deserves the same respect) and also a number of techniques for handling e-mail volume – such as only checking e-mail at set times daily.

Filing e-mail

Because e-mail records must be treated with the same care as other documents, it is essential that they are filed in the same way and the same retention rules are applied. In practice, this requires both a clear policy for e-mail storage and the tools to do the job efficiently.

The IRMS Toolkit suggests two options: print it out or save it as an electronic file. Both of these methods avoid the e-mail system being used as a long term store, which is sensible, but each presents problems.

Printing

Obviously, printing costs money and e-mail is no exception – doubly so when you then get a reply and have to print that e-mail as well. Arena often undertakes archive conversion projects (digitising an archive of paper documents) where up to half of the documentation is made up of printed e-mails – documents which were digital to start with.

A further hidden cost is that e-mails typically include some colour (signature lines, URLs, addresses) and if you're not careful this can lead to e-mails being printed as colour documents – even more expensive. Regardless of this, printing should really only be considered if you have to file emails in existing paper files. You might also consider print control software and setting defaults on your machines to restrict colour and single-sided printing, which can deliver significant savings.

Electronic filing

The second alternative suggested by the IRMS is to save e-mails to disk, outside of the e-mail system, using the 'Save As' function. This has the added benefit that the e-mail will be held together with any attachments – as it should be, to maintain a complete record of the discussion.

However, this also has a drawback; saving files in the standard '.msg' format (if you use Microsoft Outlook) means that you'll need Outlook to open those files again in the future. This is likely to be fine for a few years but probably not if the record has to be kept for many years – such as until the former pupil has reached 25 or 30 years of age. When capturing the electronic archives of organisations, we have encountered several cases of obsolete file types used with older programs such as WordPerfect (anyone remember it?) which dates back as far as the mid-1990s.

The alternative

A better solution is to make use of an appropriate Electronic Document and Records Management System (EDRMS). A good system will provide the following features which are really key to good e-mail management:

1. ***Efficient tools for storing e-mails.*** Ideally buttons within the e-mail client or quick links from the computer desktop that enable a user to file an email in the correct place within the EDRMS very quickly; i.e.; with minimal mouse clicks and typing.

2. ***Maintaining integrity of the record.*** The e-mail and any attachments should be held together.

3. ***Management of file formats.*** Emails are converted to a long-term archive format, such as PDF/A standard. This will avoid creating a store of information which you can't read in the future.

And of course, use of an EDRMS will bring the same benefits as those enjoyed for scanned information. A proper document classification policy allows retention rules to be implemented and the e-mail is managed for the whole of its relevant lifecycle. In this way, e-mails regarding students are managed according to the rules for that type of content, as are financial records and all the other types of record created by the school.

Whichever option you choose, it's crucial to enforce a robust records management policy, to ensure that emails are treated in the same way as other document types, and filed outside of the personal inboxes of your employees.

Monitoring

Because e-mail is an IT application, it is possible to monitor how it is being used and even to automatically create an indexed copy of all e-mail traffic to allow searching and analysis. Doing this provides the school with the capability to protect against a number of risks.

However, it is essential to clearly document how this monitoring will be done and how the information may be used, in order to enable the school to evidence that it has the consent of staff, students and everyone else using the e-mail system. This can be a sensitive subject which introduces an associated 'Big Brother' perception. However, it is the best practice and there is an excellent guide from the Information Commissioner's Office (ICO) as to how to do this in an appropriate and compliant manner.

Another potential use of e-mail monitoring is to tackle cyber bullying. With a captured archive of e-mail, it is a simple matter to create a searchable text-index of all the e-mails which were sent or received by your student e-mail server. This archive can then be interrogated for key phrases or messages between particular individuals.

> ***Saving files in the standard '.msg' format (if you use Microsoft Outlook) means that you'll need Outlook to open those files again in the future. This is likely to be fine for a few years but probably not if the record has to be kept for many years.***

Three ways to reduce e-mail dependence

As mentioned earlier, large amounts of e-mail (like the 80-100 items I receive on an average day) can be a source of stress. I'd like to share a few simple tactics I've used to manage e-mail in an efficient way.

- **E-mail is an "asynchronous" tool**

  There is no need to respond immediately. Turn off or ignore the pop-up icons and deal with your e-mails at a few set times each day. Interruptions are terrible for productivity, so don't create them by reading each e-mail as it arrives. If there is something really vital, the sender should really be phoning you – I've put this to the test and the "red exclamation" e-mails are always followed up by a phone call if they really are that urgent! But do set aside some time to respond to e-mail in a timely fashion.

- **Consider if e-mail is the best form of communication.**

  Would a phone call be better? Or even a face-to-face meeting? Often, one conversation can take the place of several e-mails.

- **When sending an e-mail, clarify your preferred response.**

  At Arena we have a standard of starting the subject line with "Action", "Feedback", "Info", "Review" or "Recreational", which gives a clear steer as to the expected next step. However, please do consider your organisational culture before following this guidance!

Records Management in Schools Part 6: **Risk and Disaster Recovery**

The 7th principle of the Data Protection Act (1998) is quite clear on the obligations with regard to data security and risk: "Appropriate technical and organisational measures shall be taken against unauthorized or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data."

The IRMS Toolkit makes the very valid point that: "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."

Clearly, compliance with this legislation requires on-going management of the risks to your information stores and how these risks will be mitigated. These obligations can be covered by appropriate use of technology but only once the underlying business needs have been appraised. A first step is an information audit, as described in a previous article in this series, upon which risk assessments and mitigation plans can be created.

> ***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.***

Risk assessment

Step 1: Three important questions

A good place to start with risk analysis is to look at each type of information identified in the information audit with three questions in mind:

- **Event: What might happen to this information?** Think about how the information is stored. Could it be lost or destroyed in its current form (is paper at risk from fire or flood; could electronic files be lost if the server crashes)? How might the information 'leak' out of the organisation (theft, USB stick loss, unauthorised disclosure, e-mail to the wrong person)? This question should identify a number of risks against each specific piece of information.
- **Probability: How likely is this to actually happen?** For example, a fire is a fairly unlikely risk.

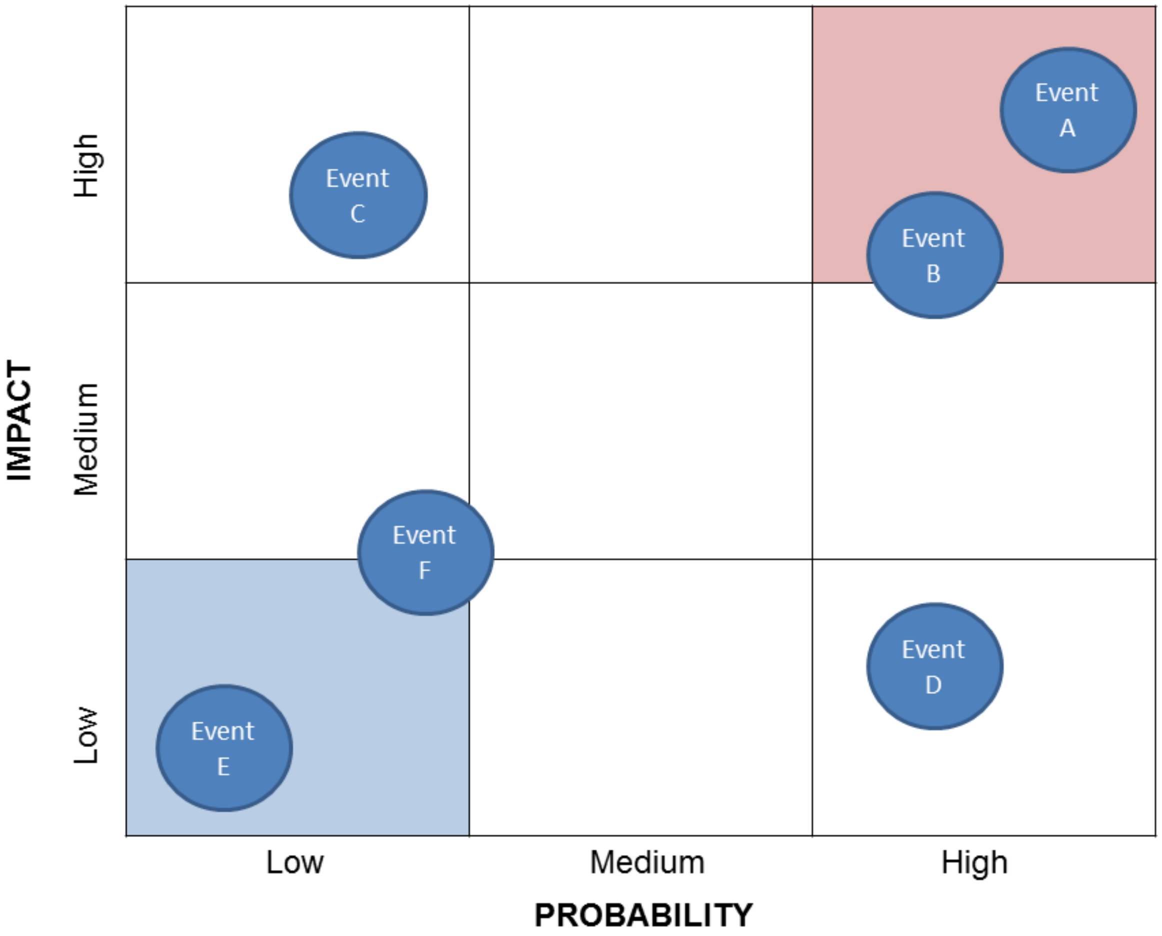
However, if you store data on USB disks, it is fairly likely that someone will lose one.

- **Impact: What would be the impact?** Some risks have bigger impacts than others. If you can't locate a permission slip, then you can ask for another to be created – a low impact event. However, if someone has left an SEN file on the bus, that's a serious problem.

Step 2: Plot your risk priorities

When you have this information, categorise each event by its probability and impact (low, medium or high) and plot each event onto a grid with probability on the x-axis and impact on the y-axis. Key issues will appear in the top-right, giving you a good appreciation of your risk priorities and where to start.

Take care not to neglect events which may be unlikely but would have a very serious impact; these "Black Swan" events will still need some thought, prevention and possibly even a coping strategy.



Step 3: Mitigation plans

The next step is to consider risk mitigation – what can you do about some of these risks to reduce their impact or remove them altogether?

The IRMS Toolkit describes a number of mitigations to general IT risks including off-site and secure backups, password policies and having no fragile or sensitive data stored on local PCs or laptops. This is all essential.

The Toolkit also discusses the risks associated with loss of paper documents in a flood or fire and the benefits of metal cabinets over open shelves, as well as the need for auditing of paper file locations and clear desk policies. These are, again, all essential if using paper files – but these steps only mitigate the risks, rather than removing them.

The application of an appropriate Electronic Document and Records Management System (EDRMS) can remove the risks to physical paperwork, by removing it, and placing the information archive into the protection of IT mitigation procedures. If this is done, information stores such as pupil files are covered by the same processes and policies as any other IT backup – greatly reducing risks and saving time by covering a multitude of risks together. An EDRMS can also provide access security and auditing, thereby removing many data breach risks.

Continuity planning

Having undertaken a risk management exercise, determined impacts and mitigated as much as possible, the next step is to compile a list of actions which will be taken should the worst happen – and in what timeframes.

Again, this builds on the information audit and the key question is how quickly does each classification of information need to be made available again? Once this is understood, the order of restoring IT systems (typically) can be defined – and then this should be subject to some real-world thinking as to whether it is practical. For example, if a file server contains information which is required to be made available within 24 hours of a server failure, can the backup be restored to a spare server or does a new server need to be procured? If a new server is required – maybe the spare server is also likely to be destroyed? – then there needs to be a plan for how this will be achieved to meet the overall elapsed time requirement.

Without testing, you have no assurance that the plan is complete, actionable and up-to-date.

Test, test and test again…

A continuity plan is something you hope never to need. But it must be tested – and that testing should be regularly repeated. Without testing, you have no assurance that the plan is complete, actionable and up-to-date. This can be a painful and time-consuming process but it's just not possible to write a plan which is error-free, and you don't want to meet the problems when you are already in the midst of a crisis.

When the worst happens

Sadly, Arena has seen cases where large amounts of paper documents have been lost. Examples include fires destroying buildings used for information storage, floods wiping out basement archives and even leaky roofs causing irreparable damage. We’ve also seen a surprising number of servers lost without an up-to-date backup being available. In most of these cases, a major impact has been suffered because a thorough risk assessment and/or regular process checking were not done. Having said this, some events were acknowledged as low-probability/high-impact risks against which the organisation had taken a conscious and calculated risk.

The IRMS Toolkit states that an individual should be appointed as the "named member of staff to liaise with the Information Commissioner’s Office in the event that a major information breach needs to be reported". We hope that by following these guidelines, and by using appropriate technology, this named person will have no need to speak to the ICO!

Arena currently works with over 750 education sector clients, helping them with the common issues they face relating to documents. We provide the hardware, software, service and expertise that enables organisations to cut costs, improve efficiencies and become greener.

mstore for Education is our own electronic document and records management system (EDRMS).

mstore for Education delivers a user-friendly mechanism to improve the whole document storage, retrieval and archiving process, whilst adding a level of security and functionality to improve legal compliance and the security of critical files.

Benefits of mstore for Education:

- **Legal Compliance:** used in accordance with an appropriate records management policy and procedures, **m**store enables compliance with sector best practice and legislation including BSi10008, the Freedom of Information Act 2000, Data Protection Act 1998 and Public Records Acts 1958/1967.

- **Safeguarding: m**store audits who has viewed information and tracks user activity without deleting original files. Users can be given different levels of access, providing you with a high level of security.

- **Accessibility:** Any document can be filed in **m**store, including emails. Records are kept together in one central location, creating an efficient way to share documents and preventing loss.

- **Document retention and archiving:** **m**store records expiry dates, ensuring all records are up to date for audits, including OFSTED inspections. Documents that have reached the end of their retention period can be flagged for deletion.

- **Decreased copy and print volumes:** a reduction in the circulation of paper documents naturally reduces print and copy to help you to meet your sustainability goals and reduce related costs.

- **Disaster recovery:** Documents are protected from loss through fire, theft, flood and malicious intent.

- **Efficiency:** Working with electronic documents instead of paper reduces time associated with filing, retrieving, sharing, processing and archiving documents.

> *"Arena has transformed the way we work with documents; they have delivered so many positive outcomes that we wouldn't be in such a strong competitive position without them."* Ian Findlay, Bursar, Bradford Grammar School
>
> *"**m**store will deliver excellent value for money - I have already recommended it to other schools. It handles every aspect of document management that a school could need while still offering an affordable solution. A one hour demonstration will be all it takes to convince you!"* Jacqueline Waters, Director of Business and Finance, Appleton Academy
>
> *"**m**store has made the processing of our pupil records much more efficient. We've gained valuable time and storage space, we are dealing with less paper and we feel confident that our documents are very secure."* Ian Parnaby, Business and Community Leader, York High School