Information Management Handbook for Schools

London Borough of Barnet

Document Name	Information Management Handbook for Schools		
Document Description	This document is intended for use by Barnet Borough Schools. It provides guidance to schools and highlights key information management areas of responsibility.		
Document Author 1) Team and 2) Officer and contact details	1) Information Management Team 2) Lucy Martin, lucy.martin@barnet.gov.uk ext: 2029		
Status (Live/ Draft/ Withdrawn)	Live	**Version**	01.00
Last Review Date	New Doc	**Next Review Due Date**	Dec 2017
Approval Chain:	Head of Information Management	**Date Approved**	Dec 2015

Version control

Version no.	Date	Author	Reason for new version
V01.00	14-08-15	L Martin	New document

Contents

1. Introduction

The aim of this Handbook is to bring together key information management guidance in one central place. It has been written in conjunction with reports and guidance issued by the Information Commissioner's Office (ICO); the UK's independent body set up to uphold information rights.

It is intended to provide practical help to schools on how to protect and appropriately manage information. The guidance specifically looks at compliance with the Data Protection Act 1998 (DPA) and the Freedom of Information Act 2000 (FOI).

The Handbook should be used as guidance only and should not be quoted as being a "standard" or "policy". Whilst Barnet Council have issued this document as helpful guidance to schools and will aim to ensure it remains as such, it should be noted that all schools, as independent public bodies, are directly responsible under the DPA for the collation, retention, storage and security of the information they produce and hold. Therefore, it is advised that you seek independent legal advice where appropriate and always adhere to school or authority approved information management policies. It is important to note that this Handbook does not cover all elements of information management or compliance, but instead touches on the more commonly raised concerns, and provides links to further information.

It is important to note that information is a strategic asset and it is important for organisations to manage it well. Information management is not just about compliance (advising on the safety and security of information) but also about managing business risks based on:

- Not knowing what information or data we have, where it is or what anyone is doing with it;
- Not knowing what information is for;
- Not being able to use information or data due to process, access and quality issues;
- Information not being available when you need it;
- Not understanding information through a lack of context and / or ownership;
- Keeping information when we don't need to;
- Costs for resolution following compliance breaches and data loss.

It is important for each school to take information management seriously and ensure there is an appropriate framework in place, which includes; policies for employees; clear lines of responsibility; guidance on where to get help and appropriate points of escalation.

Barnet Council has a suite of published Information Management policies which can be referenced by schools. The policies are the copyright of the London Borough of Barnet, but you are welcome to print and use the policies for personal use or study. However, if you wish to use a policy or part of its wording you should contact us for permission prior to using the content.

2. Data Protection Act 1998 - Overview

The Data Protection Act 1998 (DPA) is the UK law which governs the way organisations and individuals handle personal data. i.e. information that can identify a living individual.

Schools have direct responsibility for ensuring that they comply with the DPA and handle personal data in line with it. Schools should consider obtaining their own data protection and/or legal advice and formulating their own data protection, data security and data handling policies.

The DPA has eight core principles which must be adopted when handling personal data. Unless all principles are complied with you will not be fully compliant with the DPA.

These are that personal data must:

1. be fairly and lawfully processed
2. be processed for limited purposes
3. be adequate, relevant and not excessive
4. be accurate and up to date
5. not be kept for longer than necessary
6. be processed in line with the rights of individuals under the DPA
7. be kept secure
8. not be transferred to other countries without adequate protection

Schools must ensure they register with the Information Commissioner's Office (ICO) advising of the personal data processing they are undertaking. It is an offence of the Act not to maintain your registration entry and therefore you must ensure it remains up to date.

Data protection advice for schools is on the ICO website.

The DPA places a number of statutory obligations on schools. These are explained in more detail within this Handbook.

2.1. Personal and Sensitive Personal Data

Personal data is information which relates to an identifiable living individual that is processed as data. Processing means collecting, using, disclosing, retaining, or disposing of information. The data protection principles apply to all information held electronically or in structured files that tells you something about an identifiable living individual. The principles also extend to all information in education records. Examples would be names of staff and pupils, dates of birth, addresses, national insurance numbers, school marks, exam results, assessments and staff development reviews.

Sensitive personal data is a sub category of personal data and is information that relates more specifically to race and ethnicity, political opinions, religious beliefs, membership of trade unions, physical or mental health, sexuality and criminal offences.

The difference between processing personal data and sensitive personal data is that there are greater legal restrictions on the use of the latter. Whilst care should always be taken over the security and confidentiality of all personal data, additional care and often

a higher level of security should be applied when handling sensitive personal data. You will hold sensitive personal data in pupil and staff records so you need to be aware of the extra care it requires.

You also need to differentiate between personal information that individuals would expect to be treated as private or confidential (whether or not legally classified as sensitive personal data) and personal information you can make freely available.
Example: the head teacher's work email address whilst it may constitute personal data, appears on public documentation and therefore would not be considered private. However, the head's own home email address would usually be regarded as private information.

The DPA requires you to strike the correct balance in processing personal information so that you respect individuals' privacy where it needs protection. The eight data protection principles are the key to finding that balance and ensuring compliance with the DPA. All schools should be aware of these principles. Most schools now use an electronic information management system and electronic communication, and many operate their own websites. Electronic processing of personal information is therefore the norm; however, schools are also likely to hold some information on paper.

2.2. Privacy Notices

Being "fair" in the processing of personal information (1st Principle of the DPA) means being clear and transparent about how you will use the personal information you collect. To comply with the first and second principles of the DPA, you should have in place a 'fair processing notice', sometimes referred to as a privacy notice.

You should give a fair processing or privacy notice to parents and pupils before or as soon as you obtain their personal information. The DPA does not proscribe a privacy notice's format – it could be in a school prospectus, an information pack, on a website or in a separate document. If you record personal details for specific purposes, say for counselling, you may need a privacy notice specifically for that process on top of your normal privacy notice.

Schools must ensure that all parents and pupils are issued with a fair processing notice. This must also cover any data sharing activities that the school enters into with other organisations such as the local authority.

The ICO maintains a "Privacy notices code of practice" which is located on its Privacy by Design webpage. The Department for Education has also issued guidance regarding privacy notices on their website.

2.3. Data collection and use

Personal data should only be collected, retained and used where it is necessary and justifiable to do so. It should also be kept up-to-date and accurate.

- You should not collect or retain personal data "just in case". Information should not be retained or collected purely because you think it will be useful in the future.
- Do not email entire spreadsheets to colleagues when only a column or two of information is required – remove what is not necessary

- Do not email more people than necessary, only email those with a genuine need to know. If you are in an email chain, check each time whether everyone in the chain still needs to be included in your reply.
- Consider anonymising information ahead of sending – do you really need to send personal details?
- The responsibility for data quality should be clearly assigned and everyone must understand their individual responsibility in respect of data quality. When you are notified of any changes/amendments to personal data these must be updated immediately to avoid information becoming inaccurate and out of date. Any other copies of the data must also be updated.
- You must take reasonable steps to ensure the accuracy of any personal data you obtain, especially if you are planning to act on it or pass it on to another person;
- Ensure that the source of any personal data is clear;
- Carefully consider any challenges or obstacles with regards to maintaining accuracy of information; and
- Where information has been shared with others, you have a responsibility to ensure they are notified of any changes, so their records can also be updated.

2.3.1. CCTV

As CCTV captures and / or records images of identifiable individuals the processing of this information is covered by the DPA. It is the school's responsibility to ensure it complies with the CCTV Code of Practice and ensure necessary safeguards are in place with regards to access and use of footage.

You must make sure your DPA register entry with the ICO is up to date and clearly states the use of CCTV. You should maintain appropriate signage and staff, pupils and visitors must be made aware of why you are collecting personal information in the form of CCTV images and how it will be used.

If part of the purpose is to help maintain good order in the school, you need to mention this. You should site cameras only where they are needed for the stated purpose and where they do not unnecessarily intrude on anyone's privacy.

Give some thought to why you keep any recordings as well as having a agreed retention period based on the possible need to review the footage. This retention period should be notified to those…..Also consider who is allowed access to this footage and why.

Remember that people can request CCTV images under subject access requests. See section 3.6 below.

2.3.2. Photographs

The ICO advises that schools may take photos for inclusion in a printed prospectus or other school publication without specific consent, as long as they have indicated their intentions through an appropriate privacy notice.

Take extra care if the photos to be published are of young pupils or if you intend to name individuals in a photo or put the pictures on a website.

Images captured by individuals for personal or recreational purposes, such as with a mobile phone, digital camera or camcorder, are exempt from the DPA. If a parent

makes a video of their child in a school play for their own family use, this is not covered by data protection law. A school may want to consider putting in place a policy restricting the taking of photographs or other images or to stipulate they are not published on the internet to safeguard children, but this is purely a local decision and doesn't need to be done under the DPA.

If the school itself records the school play so it can sell the recordings to parents, it needs to make sure it is complying with the DPA and that there is appropriate consent sought from those who will be filmed ahead of filming etc.

2.3.3. Websites

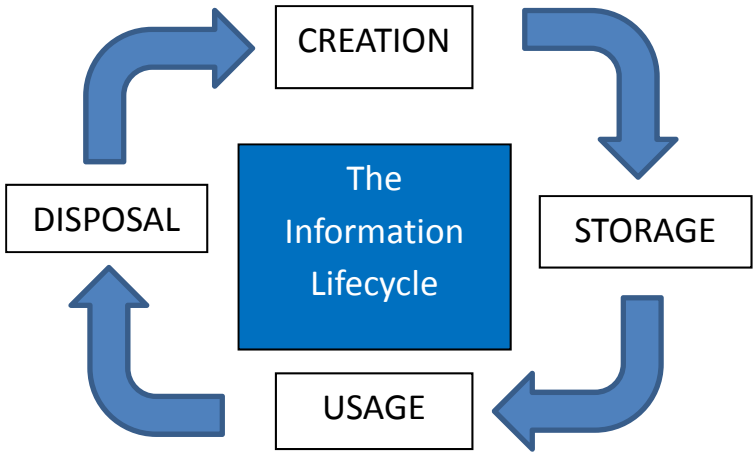
A school website helps parents and pupils view information about your school, read your privacy notice and see what information you provide under your Freedom of Information Act publication scheme. If you post personal information, including images, on webpages available to all, you must comply with the data protection principles.

The ICO has highlighted four main areas of importance that need to be considered:

- Do not disclose personal information (including photos) on a website without the individual pupil, member of staff or governor being aware. Consent should be sought before publishing photographs on a website.
- On more sophisticated websites, where access to some sections is username and password controlled, you must take care to give only the necessary level of access and maintain strong password control. If you need to restrict access to part of the website, you should adequately protect this restricted information. Giving only the necessary level of access means making checks before doing so and ensuring access is stopped when no longer needed.
- Be wary of metadata or deletions that could still be accessed in documents and images posted on a website.
- Adhere to the regulations regarding the use of cookies on websites. Refer to the ICO Guidance on "Cookies and similar technologies" for more information.

3. Data security - Overview

During the lifecycle of the data, you must ensure it is appropriately protected at all times. Where the data is being managed by another organisation on your behalf, you have a duty and responsibility to ensure you know how the data is being managed and what security has been put in place to protect it. The information lifecycle looks like this:



Appropriate security must be adopted throughout the lifecycle. Good security is often good practice and common sense.

Data security can be split into 3 broad areas of concern:

- Physical security
- Security of electronic personal data
- Security of paper-based personal data

3.1. Physical security

Physical security covers not only building security and the security of staff and pupils, but should also cover physical security of information, and restriction of access to confidential personal information.

You should regularly review the physical security of buildings and storage systems, and access to them. You should regularly consider any risks involved and consider ways of mitigating those risks. If inadequate steps have been taken for protection, this amounts to a breach of the data protection principles.

All portable electronic devices should be kept as securely as possible on and off school premises. If they contain personal information, they should be kept under lock and key when not in use. In addition to being financially prudent, this is also legally required if they hold personal information that could be considered confidential.

3.2. Security of electronic personal data

3.2.1. Passwords

Strong passwords should be encouraged if any electronic equipment holds confidential personal information.

Passwords must be at least 8 characters in length and should include a mix of upper- and lowercase letters, as well as numeric and other characters (such as # @ $ *). Obvious passwords are to be avoided (e.g. date of birth, name of pet, children, last holiday destination). The ICO also recommends you set up a regular prompt to change your passwords and use different passwords for separate systems and devices.

Passwords are the responsibility of individual users; they **must not** be used or shared with anyone even for a short period of time. By not sharing passwords you are protecting against providing someone with unauthorised access to information or systems they should not have access to.

3.2.2. Encryption

Encryption software should always be used to protect all portable devices and removable media, such as laptops, tablets, BlackBerrys and USB devices, which hold or have the ability to access personal information.

Encryption software uses a complex series of algorithms. The information on an encrypted drive is hidden from any unauthorised individuals who lack the pass code or key to the algorithm. Since encryption standards are always evolving, the ICO recommend that data controllers ensure their solutions stay up to date and meet generally accepted standards.

3.2.3. Placement of computers

Where computers are kept in public places, the screen should be away from public view where possible. For example, it should not be possible to see computer screens in the school office from public areas where parents or contractors visit. Machines should be locked (password protected) whenever they are unattended.

Workstation screensavers should also be configured to automatically lock after a short period of inactivity.

3.2.4. Email

Email is often not deemed a secure method of communication as content is easily copied, forwarded, archived or intercepted. Those advising on best practice as far as information security is concerned, warn against using email for confidential communications.

Schools often use email to contact parents. As a way of communicating general information it is cheap and convenient. But as mentioned above, it can present security difficulties if used to communicate confidential personal information.

Circular emails to parents should be sent bcc (blind carbon copy) so that email addresses are not disclosed to everyone.

You should also check (and check again) that an email is going to the correct email address and that you are sending only the information that needs to be sent. If in doubt send a test email first. Do not guess an email address but check first, in case an organisation has more than one person of the same name working for them for example. Always remember to check the content of email attachments before hitting send.

Sensitive personal data should never be sent by normal email unless the content has been appropriately encrypted, via a secure method of email. Schools wishing to share personal or confidential data with the Local Authority can use USO-FX (provided they have bought into LGfL). Schools are responsible for ensuring they have appropriate methods of secure email transfer in place.

3.2.5. Data servers

Consider who manages your data servers, and know where your data is stored. Are servers being appropriately maintained, kept up to data with appropriate security and virus definitions? As a data controller you have responsibility for gaining assurances from your IT provider that necessary data security is being implemented and ensuring you are happy with the processes being undertaken.

Ensure system access is always checked, audited and up to date.

If your systems are externally hosted be sure to gain assurances about where data is stored. Quite often hosted systems or servers or even the back-up facilities are located outside of the EEA (European Economic Area). Additional measures need to be taken in these cases. See reference to Principle 8 of the DPA on the ICO website.

3.2.6. Cloud storage

Knowing whether to use cloud storage, which provider to choose e.g dropbox, google docs, amazon cloud etc, and how to understand whether data is secure can often be very confusing.

The Department for Education has made available some guidance on this very matter, which has been designed to help schools in understanding the complexities of cloud storage.

https://www.gov.uk/government/publications/cloud-software-services-and-the-data-protection-act

3.3. Security of paper-based personal data

Whenever possible, paper records should be kept to a minimum. Storage rooms or lockable cabinets should be used to store paper records.

Papers containing personal information should not be left on office and classroom desks, on staffroom tables or pinned to noticeboards where there is general access.

The main rule is to be as careful with other people's personal information as we would expect others to be with ours.

Consider where printers are located. Ensure they aren't accessible by members of the public, parents and pupils.

Make sure all paper jams are dealt with swiftly so that information is not left vulnerable, and also implement pin code printing.

Consider what information you are posting out: is the method of communication secure enough or should you be considering recorded or special delivery for more sensitive or confidential matters?

3.3.1. Secure disposal

When disposing of records and equipment, make sure personal information cannot be retrieved from them.

Paper should be shredded via a cross cutting shredder before disposal. Do not dispose of personal information in recycling bins.

De-commissioned computers and other hardware must be fully wiped before disposal. Advice can be obtained from the Information Systems department or Barnet Schools Technical Support.

3.4. Taking work home / working from home

Schools should consider implementing a working from home policy and/ or a policy on taking information off site, to ensure that staff have an understanding of their responsibilities when taking work out of the office / school environment e.g. pupil homework or assessments.

When any information that could be considered in any way private or confidential is taken from the school premises in electronic or paper format, you should ensure you have relevant authorisation and expectation requirements outlined in policy.

The policy should be clear about what can, or can't be taken offsite, and include security measures that should be adopted when storing or working on information in the home.

For example:

- Always maintain a record of information taken off site, so in the event of a loss or theft, the risk can be appropriately assessed.
- Always keep paper records separate from valuables.
- Never leave information accessible to other people. e.g. family members, visitors, or members of the public. Records must be put away in a secure cabinet in the home when not in use.
- Don't leave bags or cases containing paper files or equipment visible in a car. If it is unavoidable to leave paper records/hard-copy material in a car, lock them in the boot.
- When travelling on public transport keep your bag/case containing school assets close by at all times. Items should not be placed in luggage racks or storage areas, as this increases the possibility of theft or the misplacing of the item.

3.4.1. Use of privately owned computers or email at home

Whilst it is common for some school staff and governors to use their own privately owned computer equipment for school business, this means the school itself will have little control over the security and disposal of such equipment. If any of the school's personal information is held on private equipment and something goes wrong, the school will remain responsible unless it can prove it did everything reasonably possible to keep the information secure.

3.4.2. Transportation of data or confidential documents

You should take reasonable care to minimise the risk of theft or damage. IT equipment must be transported in a clean, secure environment. During transfer of equipment between home and work you should keep the equipment out of sight and not leave it unattended at any time. Computer equipment or manual data must not be left in your car overnight.

Ensure any encryption software is engaged and activated before you leave your place of work by fully shutting down your laptop or mobile device.

3.4.3. Storage of equipment and documents

You should take all reasonable steps to minimise the visibility of computer equipment from outside the home, and to secure windows and doors when the home is unoccupied.

You should secure confidential data or reports that you are not actively using in the most secure area of your home.

Ensure that your equipment is password protected and that your files are stored in an area not accessible to others.

3.5. Information losses & security incidents

If you have reason to believe that security has been breached and confidential data may have been compromised, the incident needs to be appropriately handled as quickly as possible.

There are four important elements to any breach-management plan:

1. Containment and recovery – the response to the incident should include a recovery plan and, where necessary, procedures for damage limitation.

2. Assessing the risks – you should assess any risks associated with the breach, as these are likely to affect what you do once the breach has been contained. In particular, you should assess the potential adverse consequences for individuals; how serious or substantial these are; and how likely they are to happen.

3. Notification of breaches – informing people about an information security breach can be an important part of managing the incident, but it is not an end in itself. You should be clear about who needs to be notified and why. You should, for example, consider notifying the individuals concerned; the ICO; other regulatory bodies; other third parties such as the police and the banks; or the media.

4. Evaluation and response – it is important that you investigate the causes of the breach and also evaluate the effectiveness of your response to it. If necessary, you should then update your policies and procedures accordingly.

Barnet council will offer initial advice to you if an incident occurs, but it may be more appropriate to seek your own legal advice.

The ICO do expect organisations to report serious breaches of the Data Protection Act to them for further investigation. Guidance on data security breach management is available on the ICO website, referenced under Principle 7 – Security.

3.6. Subject Access Request (SAR)

The Data Protection Act provides a right of access to all data subjects to a copy of all personal data a school holds about them. This is known as the Right of Subject Access and forms part of the 6th Data Protection principle. It can be exercised by submitting a written request.

It includes information in correspondence and in notes made by governors, teachers and other staff. Information can take a number of forms e.g. paper, electronic, CCTV footage, a picture or even an audio recording.

Subject Access requests have a statutory response deadline of **40 calendar days** which must be adhered to and a specific response process should be followed.

You may charge a fee for answering a SAR. There is a standard fee of £10 and a sliding scale for information in educational records. A valid SAR should be in writing, this can include email, and you should confirm the requester's identity.

Parents can make subject access requests on their children's behalf if the children are deemed not to be of and age of understanding or they have consented to their parents doing this on their behalf. If a child is capable of making a request themselves and understands the process then they should be encouraged to so this themselves. They can of course provide consent for their parent to undertake this on their behalf if they so wish. Where a child makes a request themselves all communications regarding the request should be directed to the child and not the parent(s), unless the child has consent for you to do so. There is no automatic right for a parent to have access to their child's information just because they are under the age of 18.

A subject access request may be difficult to detect as they are sometimes made as part of wider complaint letters. However, the simple rule is that if the requester is seeking information about themselves then the request is likely to fall under the SAR provisions and should be responded to accordingly.

It is a legal obligation to respond to a Subject Access request and schools should put in place a clear policy which covers how request of this nature should be handled. A clear log of the requests should be maintained and a concise note or copy of the information that is released in case a query or complaint is raised.

There are a limited number of exemptions that apply to the right of subject access. Further information can be located on the Education pages of the ICO website.

3.7. Use of service providers & contractors

When entering into an arrangement with another organisation for them to undertake work on your behalf you must ensure that:

- the third party meets an appropriate level of security
- they have been appropriately vetted
- you have the necessary written agreement or contract in place that protects yourself and any school information they may have access to (directly or indirectly).

The school will remain responsible for any processing that a service provider might do for them. Schools will therefore ensure they have undertaken necessary checks regarding reliability and ensure that appropriate security measures are adopted. Annual checks should also be undertaken to ensure agreed standards do not slip.

3.8. Information sharing & disclosures of information

All schools share personal information with other organisations. Sharing personal information involves providing it to another organisation or person so that they can make use of it.

The main organisations that schools share personal data with are:

- local authorities;
- other schools and educational bodies; and
- social services.

The three most important aspects to consider when sharing data are:

- making sure you are allowed to share it. Information sharing should only be entered into where you have a clear legal basis that allows the sharing to happen, or you have sought consent from the individuals concerned.
- ensuring that adequate security (taking into account the nature of the information) is in place to protect it; and
- providing an understanding in your fair processing notice of who is likely to receive personal information from the school.

If information about a pupil is shared with parents, sharing must be done in line with the data protection principles, and the rights of the pupil.

Similarly, sharing parent contact details with other parents in the class should be carefully considered. Have you sought consent, and are parents aware this may happen? Make sure you take into account the 3 aspects highlighted above.

3.8.1. Sharing information with key partners

There are many occasions where information will need to be routinely shared between partner organisations and / or third parties, for example, the police, other educational establishments, the NHS, or local authorities.

You must make sure that such sharing arrangements are carried out lawfully and that it is appropriate to share. This means that there must be clear legitimate reasons why the information should be shared, and all eight data protection principles must be adhered to.

As much as possible, arrangements for sharing should be formalised through an agreed and signed Information Sharing Agreement. A record of all sharing arrangements should also be kept, and agreements regularly reviewed.

Further details can be found within the ICO – Data Sharing Code of Practice.

4. Records Management

The Information and Records Management Society (IRMS) have published a "Records Management Toolkit for Schools Version 4 - May 2012" which provides guidance on a number of areas of information management specific to schools.

4.1. Records management policy

Each individual school should have a records management policy. This may be one that has been adopted from the local authority or one that has been created independently by the school.

The IRMS toolkit above contains a basic policy document which can be adopted or adapted to reflect the different needs of different schools.

4.1.1. Records management programme

The IRMS Records Management Toolkit aims to assist individual schools to manage records throughout their lifecycle. There is advice about managing email to ensure that it becomes part of the vital record. There is information and advice about information security and how to ensure compliance under the Data Protection Act 1998.

There is also guidance on business continuity requirements and advice with regards to undertaking an information audit.

4.1.2. Pupil records

Some guidelines about what should be included in the main pupil record have been provided in the toolkit along with some advice about what information should be transferred on to the next school and how this information should be transferred.

4.1.3. Retention guidelines

The core part of the toolkit are the retention guidelines which list all the possible records any school, in England & Wales, might produce and the recommended retention periods. Some of these have a statutory basis, others have been agreed in consultation with schools around the county. There are also retention guidelines for Early Years Providers. There is some information about the benefits of using a retention schedule. There are also guidelines about the safe disposal of records which may include transferring records to the local archive office.

4.1.4. Closed school guidance

This section of the toolkit provides general guidance about what needs to be done with records when a school closes or amalgamates with another school in the same area.

5. Freedom of Information Act 2000 – Overview

Since 1 January 2005, there has been a legal right under the Freedom of Information Act 2000 (FOIA) for any person to make a request to a public authority for access to information held by that authority. This includes governing bodies of maintained schools and academies.

Governing bodies are responsible for making sure that their schools comply with the FOIA. They should also reassure themselves that the school has in place a Freedom of Information publication scheme. The legal presumption of openness makes it more important that a school decides its policies and conducts its day-to-day operations in a way that stands up to public scrutiny.

As requests for information can be received by any member of staff the school must ensure that all members of staff are aware of the FOIA and how the school handles requests for information.

Schools are under a duty to provide advice and assistance to anyone requesting information and must respond to the enquiry promptly, and in any event, within either 20 school days or 60 working days (whichever is shorter) following receipt of the request. The Freedom of Information (Time for Compliance with Request) Regulations as amended exclude days that are not school days from the 20 working day period.

6. Training

Many information management failures and data protection breaches are caused by a lack of knowledge and awareness and anything that promotes awareness is to be recommended. Whilst mistakes can happen they can often be prevented by making staff aware that a potential problem exists, the risk being identified and knowing how it can be mitigated.

Information management is not optional: there should be someone at, or accessible to, every school who has a working knowledge of information rights and records management linked to an understanding of the systems in use.

All staff (and volunteers and governors) should receive some guidance on confidentiality of personal information, preferably linked to written policies. Raising staff awareness on information management and data protection should be a standing item for staff meetings and training days, as well as inductions.

The ICO has a website giving advice and guidance on most things a school would need to know about data protection and freedom of information. Their helpline can also answer specific queries.

7. Handbook review

This document will be reviewed every 2 years or earlier as required by changes in legislation, web links or information developments.

Whilst Barnet Council will endeavour to ensure guidance is accurate and up to date it should be noted that all schools, as independent public bodies, are directly responsible

for their own information management processes. Therefore, it is advised that you seek independent legal advice where appropriate and always adhere to school or authority approved information management policies.

8. Credits and Further information

Elements of this document have been taken from the following published guidance:

- Department for Education – Governors' handbook
- Information Commissioner's Office website and – Report on the data protection guidance we gave schools in 2012 – www.ico.org.uk
- Information and Records Management Society - "Records Management Toolkit for Schools Version 4 - May 2012

9. Contact Information/Further Guidance

Further advice and guidance is available from:

Email: data.protection@barnet.gov.uk or alexandra.west@barnet.gov.uk

Barnet council Information Management policies can be used as a reference point are available at www.barnet.gov.uk/information-management-policies.