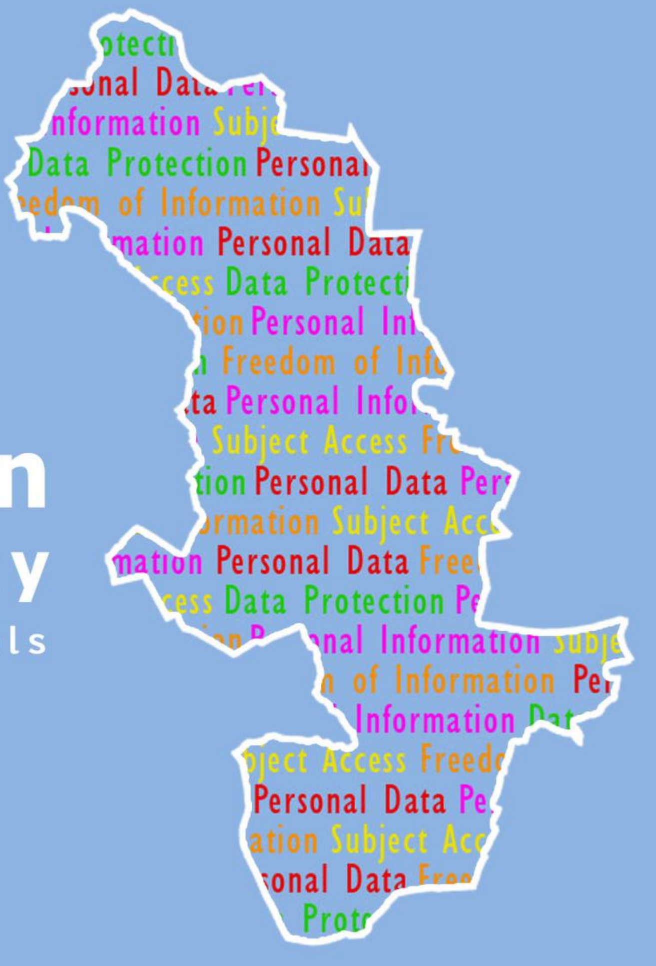
Information
and Data Security

Guidance for Knowsley Schools



Information and Data Security

Guidance for Knowsley Schools

Version 4.0

Version Control Record:

Revision	Date	Author	Summary of Changes
V1.0	19th November 2008	L Hornsby	
V2.0	18 February 2010.	Maria Bannister	
V3.0	18th March 2010	Maria Bannister	
V4.0	25th April 2013	Maria Bannister	Updated to include ICO guidance on legislative and technological changes.

Approved by:

	Date	**Version**
Learning Technologies Strategy Board	**25th April 2013**	**4.0**

Distribution: **All Primary Schools**
All Special Schools
All Centres for Learning

Information and Data Security: Guidance for Schools

Table of Contents

List of Appendices

1.0 INTRODUCTION

The Cabinet Office Report "Data Handling Procedures in Government" published in June 2008, stipulates the procedures that all departmental and government bodies need to follow in order to maintain the security of personal information. Given the personal and sensitive nature of much of the personal information held in schools, it is critical that these procedures are adopted there too.

The Data Protection Act 1998 (DPA) and the Human Rights Act 1998 (HRA) provide the legal framework for safeguarding privacy. The Freedom of Information Act 2000 (FOA) sets out the requirements of the public's right to know in relation to public bodies. Data protection legislation requires that organisations ensure that personal information, whether held on paper or electronically, is kept secure. Personal information is defined as any combination of information that identifies a living individual and provides specific information about them, their families or circumstances. This includes names, contact details, gender, dates of birth and so on, as well as other information such as academic achievements, other skills and abilities and progress in school. It may also include behaviour and attendance records.

Loss of personal information can have significant implications for the school (data controller) including interruption of service delivery, financial penalties, loss of trust and reputational damage. For the person whose information has been lost (data subject) the implications can be even more significant including financial loss, emotional distress and in extreme cases even physical harm. Sections 55A to 55E of the DPA set out a monetary penalty to ensure data controllers who do not take reasonable steps to avoid serious data breaches of the eight principles may be subject to a fine of up to £500,000 or an enforcement notice. The DPA also includes an order making power by which people who deliberately and/or recklessly misuse personal data are guilty of a criminal offence.

The protection of information (against accidental or malicious disclosure, modification or destruction) entrusted to our care is a professional and moral responsibility. It is critical that schools create and support a culture where personal information is properly valued, protected and used. This will best be achieved by implementation and regular review of information governance policies and procedures, individual accountability and staff awareness and training at all levels. Senior level ownership of information risk is a key factor in success because it demonstrates the importance of the issue. It is also critical in identifying and obtaining resource. A simple governance structure, with clear lines of ownership, is essential. Well defined roles and responsibilities are needed to follow up identified information security risks and manage breaches. Internal audit can play an important role in examining

and assuring actions taken by others. The protection of information is not a discreet role – it is the responsibility of everyone who handles it.

2.0 SCOPE OF THE GUIDANCE

2.1 Schools as "data controllers" are legally subject to the requirements of the Data Protection Act 1998. Data controller means a person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any person data are, or are not to be, processed. The DPA covers the collection, storing, editing, retrieving, disclosure, archiving and destruction of personal information. Collectively, these ensure the protection, integrity and appropriate access to and sharing of school information assets. These information assets may include information about current, past and prospective employees, pupils, suppliers, clients and others. This personal information must be dealt with lawfully, correctly and in compliance with the DPA. This guidance is to support schools with these responsibilities and in doing so will ensure the protection of confidentiality, integrity and appropriate availability of school information assets.

2.2 The guidance has been provided to all schools within the borough of Knowsley. Principals, Head Teachers and Governors are responsible for the adoption of the guidance as the School Information and Data Security Policy, its implementation, subsequent compliance and review. A specimen Data Protection Policy to underpin this guidance is attached as Appendix 1.

3.0 THE ROLE OF THE INFORMATION COMMISSIONER

The role of the Information Commissioner and his office (referred to as the ICO), is to uphold information rights in the public interest, promoting openness by public bodies and data privacy for individuals. The ICO rules on eligible complaints, gives guidance to individuals and organisations and takes appropriate action when the law is broken. While the remit of the ICO is broad, the main duties can be summarised as:

- Maintaining a register of data controllers
- Monitoring compliance (timeliness of responding to freedom of information requests and subject access requests)
- Handling complaints
- Providing support and guidance to organisations

- Taking action against organisations. Enforcement can include criminal prosecution, non criminal enforcement and audits of organisations. The ICO has the power to serve a monetary penalty – currently up to £500,000.

3.1 What the Information Commissioner Says to Schools:

The ICO published a report on the data protection advice given to schools in 2012. In summary the recommendations were:

- **Notification:** make sure you notify the ICO accurately of the purposes for your processing of personal information.

- **Personal information:** recognise the need to handle personal information in line with the data protection principles.

- **Fair processing:** let pupils and staff know what you do with the personal information you record about them. Make sure you restrict access to personal information to those who need it.

- **Security:** keep confidential information secure when storing it, using it and sharing it with others.

- **Disposal:** when disposing of records and equipment, make sure personal information cannot be retrieved from them.

- **Policies:** have clear, practical policies and procedures on information governance for staff and governors to follow, and monitor their operation and effectiveness.

- **Subject access requests:** recognise, log and monitor subject access requests.

- **Information sharing:** be sure you are allowed to share information with others and make sure it is kept secure when shared.

- **Websites:** control access to any restricted area. Make sure you are allowed to publish any personal information (including images) on your website.

- **CCTV:** inform people what it is used for and review retention periods.

- **Photographs:** if your school takes photos for publication, mention your intentions in your privacy notice.

- **Processing by others:** recognise when others are processing personal information for you and make sure they do it securely.

- **Training:** train staff and governors in the basics of information governance; recognise where the law and good practice need to be considered and know where to turn for further advice.

- **Freedom of information:** after consultation, notify staff what personal information you would provide about them when answering FOI requests.

The information provided in this guidance supports schools with these responsibilities.

4.0 DEFINITION OF DATA

Data is any information, including electronic capture and storage, manual paper records, video and audio recordings. Any images, however created are included. Schools hold personal information on learners, staff and other people to conduct day to day activities. Some of this information could be used by another person or criminal organisations to cause harm or distress to an individual or individuals. The loss of personal information could result in adverse media coverage and reputational damage and potentially legal action and financial sanction. Every member of your school, irrespective of their employment status (and others who are contracted to act as agents for the school) has a shared responsibility to secure any personal or sensitive information used in day to day professional duties. The secure handling of information is everyone's responsibility – whether they are an employee, consultant, software provider or managed service provider. Failing to have proper controls in place makes the information, the data subject and the school as data controller vulnerable.

5.0 MAIN REQUIREMENTS OF THE DATA PROTECTION ACT (1998):

The ICO plays a statutory role in ensuring compliance with the DPA. The main principles are detailed below:

i. Personal information shall be processed fairly and lawfully and, in particular, shall not be processed unless –

(a) at least one of the conditions in Schedule 2 (Appendix 2) is met, and

(b) in the case of sensitive personal information, at least one of the conditions in Schedule 3 (Appendix 2) is also met.

ii. Personal information shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.

iii. Personal information shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.

iv. Personal information shall be accurate and, where necessary, kept up to date.

v. Personal information processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.

vi. Personal information shall be processed in accordance with the rights of data subjects under this Act.

vii. Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal information and against accidental loss or destruction of, or damage to, personal information.

viii. Personal information shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal information.

5.1.0 Notification: Schools are data controllers and must register their processing of personal information with the ICO and renew annually. This is known as notification and failure to notify is a offence.

5.2.0 Privacy Notices: The data subject must be made aware, at the point of collection, of the details of the information that will be held, the purpose for which the information is held and any third party with who the information may be shared. They should also be given information about how they can access information held about them. This is known as a privacy notice. Privacy notices can also be multi layered for example, a shorter notice on forms, directing them to a longer notice on a website for more information.

Privacy notices should include reference to the use of CCTV in school premises.

5.3.0 Subject Access and Freedom of Information Requests: these are covered in Section 11 of this guidance.

6.0 WHAT INFORMATION DO YOU NEED TO PROTECT?

Data protection legislation requires personal information, whether on paper or electronically, to be kept secure. You should secure any personal information you hold about individuals and any personal information that is deemed sensitive or valuable to your organisation. This includes names, contact details, gender, date of birth and so on as well as sensitive information such as academic achievements, other skills and abilities and progress in school. It may also include behaviour and attendance records. The school should identify someone who is responsible for working out what information needs to be secured – an Information Asset Owner (IAO). The role of the IAO is covered in Section 7 of this guidance.

Schools should also identify their information assets. These will include the personal information of learners and staff; such as assessment records, medical information and special educational needs information. Information assets also include non-personal data that could be considered sensitive if lost or corrupted, such as financial data, commercial data, research data, organisational and operational data, and correspondence. The 'value' of an asset is determined by considering the consequences likely to occur if it is lost or compromised in anyway, such as identity theft, adverse publicity or breaches of statutory/legal obligations. This information will form the Information Asset Register (IAR) which should be kept updated and reviewed regularly. More detail is provided in Section 7.

7.0 PROTECTING INFORMATION

7.1.0 Information Governance – Roles and Responsibilities

To ensure that information is adequately protected it is critical that the school creates a culture that properly values, protects and uses information appropriately. Information governance includes responsibility to ensure policies and procedures, performance measurement controls and reporting mechanisms to monitor DPA compliance are in place and in operation across the school. Although the Principal or Head Teacher has ultimate responsibility as data controller they need to be supported in this by an information governance structure with clear lines of responsibility. This governance structure should be headed up by a Senior Information Risk Owner (SIRO).

7.1.1 The role of the Senior Information Risk Owner (SIRO) is:

- Leading and fostering a culture that values, protects and uses information for the success of the school and benefit of all who need to access it
- Owning the school's information risk and incident management framework;

- Championing the school's information security policy and information management processes and ensuring compliance by IAOs and IAAs.

- To ensure an Information Asset Register (IAR) is in place and to appoint Information Asset Owners (IAOs) for each information asset.

7.1.2 The role of the Information Asset Owner (IAO):

The school should designate someone who is responsible for working out exactly what information needs to be secured and the measures in place to do so. This is the Information Asset Owner (IAO). It may be necessary to have more than one IAO and schools may decide to have an IAO for each asset or group of assets as appropriate. For example, the organisation's management information system should be identified as an asset and should have an IAO.

The role of an IAO:

- Support the SIRO to foster a culture that values, protects and uses information

- Know what information is held within the school

- Know who has access to information assets and why, and ensure access is monitored, controlled, and compliant with policy

- Ensuring that information is shared appropriately and transferred securely

- Understand and address risks to assets, and provide assurance to the SIRO

As a result, the IAO is able to manage and address risks to the information and make sure that information handling complies with legal requirements. There may be several IAOs within a school, whose roles may currently be those of e-safety co-ordinator, ICT manager or information management systems manager.

The IAO needs to be of sufficient seniority to ensure compliance with DPA requirements. They should understand what information the school needs to handle, how the information changes over time, who else is able to use it and why. They should also understand the arrangements that need to be in place to share information appropriately and securely. They do not necessarily have to undertake the operational tasks, but they do need to ensure measures are in place to protect information and that the effectiveness of these measures is regularly reviewed. The IAO should be supported by designated a Information Asset Administrator/Administrators who have responsibility for specific information assets.

7.1.3 Information Asset Administrator (IAA):

The IAA works with the IAO to ensure effective management of the information assets they are responsible for.

The role of the IAA:

- The operational management of information assets on day to day basis, ensuring that access controls are in place and policies and procedures are adhered to.

- Ensuring that information is only shared where it is appropriate to do so, that information agreements are in place as required and that the information shared is fit for the purpose and not excessive.

- Ensure information asset registers are accurate, maintained and up to date

- Recoginising potential or actual information security incidents, initiating reporting and actioning mitigiation plans

7.1.4 Information Asset Register (IAR):

The IAO has responsibility for documenting the information that is held and the measures in place to protect it; this is the Information Asset Register (IAR). An IAR is a mechanism for understanding and managing an organisation's assets and the risks to them.

Information can exist in a diverse variety of forms but what the information is about is more crucial than the physical or electronic format in which it is held. Information assets have the following characteristics:

- They support the delivery of the school's priorities,

- They provide evidence of activities,

- Failure to protect them may have an adverse effect on the school's ability to deliver. Their use, misuse or loss may have an impact on others outside the school (including pupils, staff, families and so on).

Schools should identify their information assets which will include personal information of learners and staff (i.e. assessment records, medical information and SEN information). Information assets also include non personal information that could be considered sensitive if lost (i.e. financial data, commercial data, and research data and correspondence). The SIRO should ensure that the IAR is reviewed, updated and maintained. It is a critical document that should be included in the school business continuity plan.

7.2.0 Training and Awareness

The effective management of information is not a discreet role - it is the professional and moral responsibility of everyone who works in the school. It is therefore essential that the school leads from the top and that the provision and monitoring of staff data protection training and the awareness of data protection requirements relating to their roles and responsibilities is given high priority. Training, alongside information governance and clear policies and procedures will ensure a culture where staff are able to access to the information they need, that the information is valued and that it is protected.

7.3.0 Organisational Measures to Protect Information

To adequately protect information, organisations may need to make operational and technological changes. Some can be achieved quickly with existing resources; others will require extra investment and the help of IT and managed service suppliers. In any given organisation, IAOs will need to work out the level of change required by carrying out a thorough information risk assessment. Organisations may also need to make staff more aware of information security through training. They may also need to put in place systems and procedures for:

- protectively marking information
- encryption
- responding to security incidents
- secure remote access (using two-factor authentication where needed)

It is not possible to include detail of every aspect of protection in this guidance but particular consideration should be given to the following areas:

7.3.1 Records Management (manual and electronic): The school must ensure that processes are in place for managing both manual and electronic records containing all information. This will include having controls in place to monitor the creation, maintenance, storage, movement, retention and destruction of records containing personal information. More detail is provided in Section 8.

7.3.2 Protective Markings: It is good practice to protectively mark personal information. This will help people handling it understand the need to keep it secure and to destroy it when it is no longer needed. This is especially important if personal information is included in a report and printed. There are different levels of marking depending on how sensitive the information is.

7.3.3 Access to Information and Access Control: Passwords are important in protecting information. Knowsley Council has implemented a complex password process which supports improved security on devices accessing the corporate network. However, it is important that passwords are easy to

remember but hard to guess. It is good practice to have a password that has eight characters or more and contain upper and lower case letters, as well as numbers. Passwords must not be shared with anyone else, written down, used for personal on line accounts or saved in web browsers. Passwords must never be emailed to someone else.

7.3.4 Device hardening: It is critical that your school network is protected against malicious virus attacks and the importance of having the right technical support in place cannot be under estimated. Computers need regular updates to their operating systems, web browsers and security software (anti-virus and anti-spyware). The Learning Technologies Strategy Board (LTSB) has approved the Network Standards Guidance to support schools with this. The document includes standards for ensuring the correct policies are in place to keep computers up to date with the latest security updates. Devices connecting to the corporate network must comply with these standards. Security features installed on devices should never be turned off or bypassed. It is also important that only approved and licensed software is installed and that any unused software is removed to minimise security risks. Remember one device can infect a school network.

7.3.5 Email: Staff are provided with an approved email address in the format of "@knowsley.gov.uk" or "@staff.klear.org.uk" these must be used to conduct official business. Non approved email accounts must not be used to conduct official business because the security or location of servers cannot be guaranteed. All emails that represent aspects of official business are the property of the business and not the individual.

7.3.6 Websites: A website says a lot about a school and in many cases is the first point of contact for parents and prospective parents. Is provides 24/7 access to information about the school and a good website provides valuable information including the privacy notice and publication scheme. If personal information, including images, are posted to the school website it must be done in compliance with the data protection principles. Important considerations include:

- Do not disclose personal information – including images – without consent.

- On websites with controlled areas, ensure that the access is appropriately restricted (including removing access when it is no longer required) and strong password control is enforced.

- Be aware of metadata or deletions that could still be accessed in documents and images posted online.

Please see the link to Personal Information Online in the useful links section of this guidance.

7.3.7 Cookies: The law on how cookies and other similar technologies changed in May 2011. In essence the change means that cookies or similar technologies must not be used unless the user is provided with clear and comprehensive information about the purposes of the storage of the information and they give their consent. If you intend to use cookies or other similar technologies on your website you must take account of the principles of the DPA. Guidance has been provided by the ICO and is accessible in the useful links section.

7.3.8 Photographs: The subject of photographs in relation to DPA is often misunderstood. Schools are able to take photographs for inclusion in a printed prospectus or other school publication without specific consent as long as they have indicated their intention to do so. Extra care is needed if the photographs to be published are of young children or if the individuals are to be named. Caution should always be exercised if the photographs are to be published on a website.

Images taken for personal or recreational use are exempt from the DPA. If a family want to record a school activity involving their child the DPA does not prohibit them from doing so, although the school may have a policy in place to prevent this for safeguarding or other reasons.

If the school want to record an activity to sell on to families, they must ensure they are complying with the DPA.

Further information from the ICO on taking images in school can be accessed through the useful links section of this guidance.

7.3.9 Social Networking: Schools are well informed and proactive in promoting eSafety and will have acceptable use policies in place. However, there are potentially problems with the emerging use of Social Media for business purposes including issues related to recruitment, selection, workplace monitoring and the blurring of personal and business use. While the law does not prevent organisations from recruiting via social networking platforms, demanding access to a social networking profile would attract the interest of the ICO. Guidance is available in the ICO's Employment Practices Code (see useful links). The blurring of personal and professional use of social networking is particularly problematic and schools should review their existing Acceptable Use Policy to ensure it is explicit about requirements. An alternative is to have a separate and specific Social Networking Policy which is reviewed regularly.

7.3.10 Encryption: To comply with the intent of data handling procedures and practice in Government:

- Users should not remove or copy personal or sensitive personal information from the school unless there is a business need, they have

permission and the media is encrypted and is transported securely for use/storage in a secure location.

- Authorised users accessing data from outside the school premises must do so by secure means.

- Users must protect all portable and mobile devices, including media, used to store and transmit personal information using approved encryption software.

For schools, this means that they must encrypt any data that is classified as Impact Level 2 (IL2–Protect) or higher if this data is removed or accessed from outside any approved secure space. School laptops have been secured using corporately approved encryption software. Staff can check if the encryption is in place by looking at the bottom left of your laptop screen and you should see a yellow padlock. An unencrypted device is a security risk. School ICT Support will be happy to provide advice.

7.3.11 Network Storage: Even when encrypted, information stored on a laptop and removable media is vulnerable to accidental loss, theft or device failure. Information should, by default, be stored on a networked drive or portal where it can be backed up, recovered and made available to the school.

7.3.12 Cloud Computing: is defined as "access to computational resources on demand via a network". In relation to data protection, the issues aren't new. The security of the data, overseas transfer rules and outsourcing considerations still apply and the responsibility remains with the school as the data controller. It is essential that before schools enter into a contract that a thorough risk assessment in undertaken. Further information is available through the useful links section of this guidance.

7.4.0 Security of Mobile Technologies:

7.4.1 Laptops: Laptops are now a standard tool in the workplace and other devices with similar functionalities are becoming increasingly common. It is essential that the devices and the information they contain are adequately protected. As stated above, information must always be stored on a secure central server rather than locally on a device. Removable media should never be used to store information in the long term. This provides security and also provides protection in the case of device failure, damage, loss or theft. Laptops and other devices which provide similar functionality (i.e. notebooks, UMPCs etc) are by design portable and in some cases easy to conceal increasing the risk of theft. It is therefore important that the hard drives are encrypted and additionally that they are secured using a visible security lock when they are in use. Particular care should be taken when transporting devices to minimise the risk of theft. As a minimum:

Devices should always:

- be shut down using the ‘Shut Down’ or ‘Turn Off’ option
- when in use, be positioned to try to prevent people from seeing passwords or sensitive information on the screen and be protected by automated screenlock
- be turned off and stored securely when not in use
- protected by a physical laptop lock if available to prevent theft
- have the desktop locked (Ctl, Alt, Del) when unattended
- be protected with approved encryption software.

Staff should never:

- store remote access tokens with devices
- leave devices unattended unless security in place
- use public wireless hotspots – they are not secure
- leave devices unattended in a car unless it is unavoidable and out of sight.
- let unauthorised people use their laptop
- use hibernate or standby.

Schools should have processes in place for tracking work devices and ensuring they are signed out, used in accordance with policy and returned at the end of employment or staff relocation. Devices must be appropriately cleansed prior to reissue.

7.4.2 USB Devices (and other similar removable media): If it is absolutely necessary to use temporary storage devices these must be encrypted to FIPS 140 – 2 certification. USB devices are subject to failure, loss and theft. They should be used only when there is no other alternative. USBs should be regarded as a temporary storage method and the information saved back to the network as soon as possible. Unencrypted storage devices should never be used for the storage or transport of personal, sensitive personal or confidential information.

Schools should have processes in place for tracking the use of USBs and other removable media used by staff and for ensuring they are returned at the end of employment. Devices must be appropriately cleansed prior to reissue or disposed of securely.

7.4.3 Bring Your Own Device (BYOD): The use of personally owned devices (typically smart phones or tablet devices) for business purposes is subject to much discussion and while there are merits, safeguards need to be put in place to protect information. Use of personal devices presents difficulties and by nature these devices may be used by other members of the family. Typically, they do not benefit from encryption or other security controls and there is little, if any, control over the disposal or reallocation of these devices. Careful consideration needs to be given to the potential risks including:

- Where does the information reside?
- How is the information transferred?
- How is the device managed and controlled?
- How is the privacy of the data subject protected?
- How is information deleted and the device disposed of?
- How is compliance with policy managed?

The issues aren't new but the solutions need to be considered carefully and robustly applied. Schools should carefully consider and implement a robust security strategy and acceptable use policy before activating BYOD. The application of BYOD is relatively new and emerging but guidance has been issued by the ICO and a link is included in the Useful Links section of this document.

8.0 RETENTION OF INFORMATION:

8.1.0 Retention Periods: The DPA does not set out specific minimum or maximum periods for retaining personal data, but the fifth principle states that data should not be kept for longer than is necessary. The Information and Records Management Society gives guidance (see useful links section) and a summary document for schools is attached as Appendix 3.

8.2.0 Destruction of records: When it becomes necessary to destroy any printed or written documents containing personal, confidential and/or sensitive personal information, measures must be taken to ensure that it cannot be accessed by unauthorised parties in the future. Under no circumstances should personal, confidential and/or sensitive data be placed in general waste or recycling bins. Cross-cut shredders or confidential waste bins must be used for this type of information. Staff should be made aware of the arrangements for disposing of paper records. It is never acceptable to dispose of personal or sensitive information through domestic waste.

Schools are responsible for the information stored on computer hard drives and other removable media. Deleting files or formatting the hard drive does not provide adequate protection because it can easily be recovered using

freely available software. It is essential that equipment is retrieved when staff leave employment or are relocated and that the equipment is disposed of through approved contractors who have provided a guarantee that they will be securely cleansed and have provided a written undertaking about the process. Receipts should be obtained for all devices handed over for disposal and the school IT inventory updated. If a device is to be reissued, it must be cleansed first. Contact your IT provider for further information.

8.3.0 Remember: technical measures can only provide a level of protection. To ensure complete security there must be a school culture of information security underpinned by governance, policies, procedures and training.

9.0 BUILDING SECURITY AND CONTROL

There are of course technical measures that can be put in place to protect information. However, these cannot work in isolation and need to be underpinned by information governance, policies, procedures and training. There is also a need for staff to be aware and continually vigilant to potential weaknesses that could pose a risk. Schools should ensure that regular checks are made of the physical security measures for the building (including locks, key register, alarms and CCTV) and that reception procedures for visitors are robust and adhered too.

On site staff must always:

- wear their identification badges at all times
- ensure others use their own passes to access restricted areas (it may be polite to hold the door open but it compromises the security of the building if access isn't monitored and recorded)
- ensure only authorised people are allowed into staff areas
- lock sensitive information away when it is unattended
- use a lock for laptops to prevent opportunistic theft
- position screens and documents so that other people cannot see them
- Immediately report any concerns about security

Working offsite staff should:

- only take information that is absolutely necessary and authorised.

- ensure that information is protected offsite in the ways referred to above
- If possible, access information remotely instead of taking it offsite
- ensure paper information is transported and stored separately to laptops to add a layer of protection in case of theft
- be aware of location and take appropriate action to reduce the risk of theft
- make sure they sign out completely from any services used
- try to reduce the risk of being overlooked
- avoid the risk of conversations being overheard

9.1 **CCTV:** The ICO does not regulate the use of CCTV but does offer guidance because the use of CCTV involves the processing of personal information. Schools need to include the use of CCTV in their notification. They also need to inform staff, pupils and visitors why personal information is being collected in the form of CCTV images. Consideration must be given to where cameras are sited and how long records are kept. CCTV images can be requested under subject access requests. Further information is accessible through the useful links section of this guidance.

10.0 SHARING INFORMATION

There is a range of legislation that makes it a statutory responsibility to disclose/share information including: Children Act 1989, The Education Act 1996 (Sections 10 & 13) Crime & Disorder Act 1998, Data Protection Act 1998, Youth Justice & Criminal Evidence Act 1999, Protection of Children Act 1999, Local Government Act 2000, The Learning & Skills Act 2000, Criminal Justice & Police Act 2001, special Education Needs & Disability Act 2001, Education Act 2002, The Children Act 2004. This is not an exhaustive list and other legislation may be applicable.

Before sharing any personal, confidential and/or sensitive information with partner agencies care needs to be taken to ensure that the sharing meets the requirements of the DPA (see Section 5) and that an information sharing agreement is in place.

If a request is received to transfer personal, confidential and/or sensitive information via any electronic means (including email, FTP and CD) the necessary encryption protocols need to be verified as in place.

Information sent by fax is particularly vulnerable and this method should only be used when there is no other alternative and to not send the information would cause a serious disruption to service delivery or potentially cause harm. Schools should have a procedure in place for sending information by fax which mitigates the risk of information being compromised if it must be sent via this method.

If a request is received to transfer printed or written personal, confidential and/or sensitive information, ensure that appropriate security procedures are in place, ideally a point-to-point courier with tracking and a signed receipt by the intended recipient. If a member of your staff is delivering personal information by hand, ensure they verify the identity of who they are handing it to and get a signature.

Schools should ensure that guidance is available on who they are allowed to share information with and how to share it securely, whether the information is shared systematically or as a one off. Checklists for each of these eventualities are attached as Appendix 4 (Systematic Information Sharing) and Appendix 5 (One off Requests for Information Sharing). Requests for information and the decision should be recorded, whether information is shared or not. Examples of the way you can record this information are included as Appendix 6 (Specimen Recording a Request for Information Form) and Appendix 7 (Specimen Recording a Decision to Share Information Form).

Schools should take precautions to ensure that legitimately shared information will be handled securely by the receiving organisations; they should not assume this will be the case. Information sharing agreements are critical because they set out the rules which each organisation agrees to work by, including keeping the information secure (see section 10.2.0).

10.1.0 Data Processing Agreements: The DPA is clear that where a data controller uses a third party (data processor) to process personal information on its behalf, a written contract (data processing agreement) must be put in place to ensuring the data processer has appropriate measures in place to ensure the safety and security of the personal information. The data controller must also take reasonable steps to ensure compliance by the data processor. It is the responsibility of the data controller to ensure that information processed by third parties on their behalf is dealt with according to the data protection act, especially principle 7 ensuring the information is dealt with securely as well as with integrity and that it is destroyed within appropriate retention periods.

10.2.0 Information Sharing Agreements: Information sharing agreements can take a variety of forms and should be written to provide a framework and common understanding and agreement between parties sharing information. They should be clear, concise and relevant. Having an agreement in place does not indemnify against legal proceedings under the DPA but it does

demonstrate that measures have been taken to mitigate risk and ensure compliance with DPA principles and this would be taken into account by the ICO should they receive a complaint.

Having a clear understanding of what information should be shared, with who, when and how will ensure that schools collect and share personal information in compliance with the law, fairly, transparently and in line with the rights of the people whose information is being shared. To help with this process the ICO have issued the "Data Sharing Code of Practice". This is a statutory code (having been approved by the Secretary of State and Parliament) and explains how the DPA applies to the sharing of personal information. A link to the guidance is provided in the useful links section of this guidance and a specimen information sharing agreement containing key information to be included is attached as Appendix 8.

11.0 REQUESTS FOR INFORMATION

The processes in place to respond to any requests for personal information are covered by the DPA and are therefore regulated by the ICO. This includes requests by individuals for copies of their information (subject access requests) as well as requests for information by members of the public (freedom of information requests).

11.1.0 Subject Access Requests: The DPA gives individuals a right to access personal information held about them (unless an exemption applies). Data subjects have a right to know what information is held and to request a copy of that information. This request must be in writing (emails are included). This right may prove problematic when the data subject is a child. The ICO's guidance is that children by the age of 12 have sufficient understanding to make their own decisions but there may be exceptions to this view. Schools in any case must respond to the request within forty calendar days of receiving it. In responding to a subject access request schools must communicate the following:

- Whether any personal data is being processed;
- A description of the personal information, the reasons it is being processed, and whether it will/has been given to any other organisations or people;
- A copy of the personal information;
- Details of the source of the personal information (where this is available); and

- An explanation of any codes or abbreviations used

Schools must make a record of such requests and responses, being careful to establish the identity of the individual making the request before releasing any information to them. They must also be careful to ensure that information about other individuals is not included in the response while providing as much information as possible to the requestor.

Schools may make a nominal charge to cover the administration of such requests capped at £10.00 maximum and data subjects should be made aware of this in advance.

.

11.2.0 Freedom of Information: This act gives a right to access information held by public authorities. Under the Act schools are required to produce a "publication scheme" which is effectively a guide to the information they hold which is publically available. Schools also have to respond to individual requests (which must be made in writing – emails are included) within 20 working days of the request. There are both qualified and unqualified exemptions. The former includes reviewing the public interest test. Schools should make a record of such requests and responses.

12.0 SECURITY INCIDENTS

In the case of an information security incident or breach it is important to act quickly to mitigate potential harm or distress to individuals. There are four key stages:

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 service providers, police and the banks; or the media.

All suspected or actual breaches of data security must be reported to the School Designated Data Protection Officer and Leanne Hornsby.

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. It is also important that you have a procedure in place for dealing with any incidents and/or circumstances that do not result in breach, but could if they are not dealt with. KMBC Internal Audit Department can support you with this process.

13.0 MONITORING AND COMPLIANCE:

Schools must have an appropriate governance structure in place and ensure this is underpinned with appropriate and robust policies and procedures, training, technical controls and organisational processes. Training and awareness rising are critical to creating an organisational culture where information is valued and protected. Key considerations are summarised on the Information Security Checklist for Schools (Appendix 9).

14.0 SUMMARY:

Loss of personal data can have significant implications for the school and for the person whose information has been compromised. Data protection legislation requires that organisations ensure that personal information is kept secure and the ICO has significant powers to sanction financially or issue an enforcement notice. There is also a risk of significant reputational damage. Schools must encourage a culture where information is properly valued and protected and that each officer understands their professional and moral responsibilities. The information and guidance provided in this document supports schools in achieving and sustaining this objective.

REFERENCES:

The Information Commissioner plays a statutory role in policing compliance with the Data Protection Act, and provides advice on relevant legislation and good practice. Extensive reference has been made to the information published by the ICO in the preparation of this guidance. www.ico.org.uk

Other sources consulted:

Data Handling Procedures in Government: Final Report

Becta: Data Handling Guidance for Schools

Becta: Data Protection and Security - Summary for Schools

Department for Education: Information Sharing - Further Guidance on Legal Issues

Department for Education: Information Sharing

Brent's School Data Security Strategy

Data Handling & Security Guidance for Schools www.cambridgeshire.gov.uk

Information Security: Policy and Guidance for Schools www.wakefield.gov.uk

USEFUL LINKS - FURTHER INFORMATION AVAILABLE FROM:

ICO: The Guide to Data Protection

ICO: Report on the data protection guidance we gave schools in 2012.

ICO Guide: Privacy Notices

ICO Guide: Freedom of Information

ICO: CCTV Code of Practice

ICO Guide: Personal Information Online

ICO: Taking Photographs in Schools

ICO: Guidance on the rules on use of cookies and similar technologies

ICO Guide: DPA and School Photographs

ICO: Data Sharing Checklists

ICO: Data Protection Code of Practice

ICO: Guidance on the use of Cloud Computing

ICO: Bring Your Own Device (BYOD) Guidance

ICO: Employment Practices Guide

ICO: Personal Information Online

Records Management Society Toolkit for Schools

LINKED POLICIES:

The Operation of CCTV in Schools and Centres for Learning.

KMBC Network Standards

KMBC Email Policy

eSafety Strategy

eSafety Acceptable Use Policy

LIST OF APPENDICES:

Appendix 1

Data Protection Policy for Schools (Example)

Data Protection Policy
<Name of School>
<Reviewed: XXXX>

1. Policy Statement:

<School Name> acknowledges its responsibilities under the Data Protection Act 1998 and associated legislation. As a data controller we will take all reasonable steps to comply with our legislative responsibilities and promote good practice in the handling of information. Our actions will ensure compliance with the Data Protection Principles set down in the Data Protection Act.

This policy applies to governors, employees of the school, partner agencies and companies and contractors with who the school conducts business. It also applies to individuals who are subject to data processing by the school as part of its business.

2. Background:

We need to collect and process personal and personal sensitive information to conduct our business. This information may include information about current, past and prospective employees, pupils, suppliers and others. It may also be a legal necessity for us to collect some information to comply with the requirements of government departments. The Data Protection Act 1998 sets out the legislative framework for the handling of this information, however collected, shared and stored to ensure it is processed fairly and legally. We commit to dealing with information fairly and in compliance with the requirements of the Data Protection Act. The protection of information entrusted to us is a professional and moral responsibility of everyone who works on behalf of the school.

3. Definitions:

Data Controller	Any individual or organisation that controls personal data, in this case, the school.

Personal data (otherwise known as personal information)	Any personal information about a living person who can be identified from the information stored, for example name, address, National Insurance number, blood group and so on. This includes: merged information from other areas that the school has access to; information where an individual is identified by default - for example, there is only one female employee who works in a team; and statements of opinion about the information and how it may be used.
Sensitive personal data (otherwise known as sensitive personal information)	Personal information relating to a person's race or ethnic origin, political opinions, religious beliefs, physical/mental health, trade union membership, sexual life and criminal activities.
Data subject	This is the person who the information is about. NB: The DPA only covers living individuals.
Relevant filing system	A set of records which are organised by reference to the individual and are structured in such a way as to make information readily accessible e.g. personal records, computerised records etc.
Processing	Processing means collecting, using, disclosing, retaining or disposing of personal information. If any part of processing is unfair, there will be a breach of the Data Protection Act.

	It is considered to be processing if any of the below is being undertaken: • **H** Holding, Handling • **O** Obtaining, Organising • **A** Altering, Aligning • **R** Recording, Retrieving • **D** Disclosing, Destroying • **S** Securing, Storing

4. The Eight Data Protection Principles:

In summary, the principles are:

1. Personal information must be fairly and lawfully processed.
2. Personal information must be processed for limited purposes.
3. Personal information must be adequate, relevant and not excessive.
4. Personal information must be accurate and up to date.
5. Personal information must not be kept for longer than is necessary.
6. Personal information must be processed in line with the data subjects' rights.
7. Personal information must be kept secure.
8. Personal information must not be transferred to other countries without adequate protection.

We will:

1. Fully observe conditions regarding the fair collection and use of information.
2. Meet legal obligations to specify the purpose for which information is used.
3. Collect and process information only to the extent that it is needed for our business needs or to meet statutory requirement.
4. Ensure the quality of the information gathered and processed to ensure accuracy and relevance for purpose.
5. Apply a retention schedule to ensure information is securely disposed of in timely manner.
6. Ensure the rights of individuals to access and if necessary correct information held about them.
7. Take appropriate technical and organisational security measures to safeguard information when it is collected, shared, stored and disposed of.
8. Ensure that information is not transferred abroad without suitable safeguards.

5. Compliance Statement:

<School Name> will achieve compliance by ensuring:

1. An effective information governance framework that is reviewed regularly.
2. Ensure staff are informed of their responsibilities and trained to support them in meeting them.
3. Our technical, organisational and building security measures are robust and reviewed to test effectiveness.
4. We review our processes to ensure data subjects can access information we hold about them.
5. We review our processes for reporting concerning and addressing potential weaknesses.
6. We review our processes for ensuring compliance with our Data Security Policy.

6. Governance Structure:

An information governance structure is key to ensuring organisational processes are in place to ensure information is secure. We have adopted an information security policy which reinforces this requirement and have identified school officers to undertake these responsibilities.

Our Senior Information Asset Owner is: <name>

Our Information Asset Administrators are: <name> <record series>
<name> <record series>
<name> <record series>

7. Policy adoption and review:

A copy of this policy statement will be issued to all employees. It will be reviewed annually (or as necessary) to ensure it continues to be fit for purpose.

Proposed by (Headteacher): _____ (Sign and Date)

Adopted by Governing Body: _____ (Date)

Approved by (Chair of Governing Body): _____ (Sign and Date)

Appendix 2

Data Protection Act – Schedule 2 and 3 Conditions

Schedule 2 conditions include:

- The data subject has given consent to the data processing, or
- The processing is necessary for the performance of a contract to which the data subject is party, or for the taking of steps at the request of the data subject with a view to them entering into a contract
- The processing is necessary for compliance with any legal obligation to which the data controller is subject, other than an obligation imposed by contract
- The processing is necessary to protect the data subject's vital interests, or
- The processing is necessary for the administration of justice, for the exercise of any functions of either House of Parliament, for the exercise of any functions conferred on any person by or under any enactment, for the exercise of any functions of the Crown, a Minister or government department, for the exercise of any other public functions exercised in the public interest by any person; or
- The processing is necessary for the purposes of legitimate interests of the data controller, or of the third party or parties to whom the data is disclosed, except where the processing is unwarranted by reason of the rights and freedoms or interests of the data subject

When information is sensitive then a schedule 3 condition must also be met.

These are:

- The data subject has given explicit consent to the processing; or
- The processing is necessary for the purposes of exercising any legal right or obligation on the data controller in connection with employment; or
- The processing is necessary to protect the vital interests of the data subject or someone else, in a case where the data subject cannot give consent or consent cannot reasonably be obtained, or in order to protect another person's vital interests, the data subject is unreasonably withholding consent; or
- The processing is carried out by a not-for-profit body in the course of its legitimate activities and does not involve disclosure of the personal information to a third party without consent; or
- The processing is necessary for the purposes of, or in connection with, any legal

proceedings, obtaining legal advice or to establish, exercise or defend legal rights; or

- The processing is necessary for the administration of justice, for the exercise of any functions of either House of Parliament, for the exercise of any functions conferred on any person or under any enactment, or for the exercise of any functions of the Crown, a Minister or a government department; or

- The processing is necessary for medical purposes and is undertaken by a health professional; or

- The processing is of sensitive personal data consisting of information as to the racial or ethnic origin and is necessary for the purpose of promoting racial or ethnic equality and is carried out with appropriate safeguards.

Appendix 3

Records Management Retention Schedule for Schools

Records Management **Created April 2010**

This document has been compiled using information on retention periods from both the Information and Records Management Society and Knowsley Council policies, It is to be used when evaluating records held within schools.

Records Group	Basic file description	Retention Periods	At end of retention period	Notes
Personal records	Timesheets	End of financial year to which the records relate + 3 years	Dispose	
	Clock cards	Creation +2 years	Dispose	
	Sick notes	End of calendar year + 3 years	Confidentially dispose	
	Sickness Records:	Termination + 25 years	Confidentially dispose	
	sick pay	Termination + 25 years	Confidentially dispose	
	Staff personal files	Termination + 25 years	Confidentially dispose	
	Interview notes	Date of interview + 6 months	Confidentially dispose	
	recruitment records	Application forms for unsuccessful candidate – 6 months from date post filled. Application forms for successful candidates – add to personnel file	Confidentially dispose	

	Pre-employment vetting information (including CRB)	Keep for maximum of six months following the recruitment decision unless a dispute is raised or, in exceptional circumstances, where CRB agreement is secured	Confidentially dispose	Should be recorded for school workforce census
	Disciplinary proceedings:	-		Where the warning relates to child protection issues see below. If the disciplinary proceedings relate to a child protection matter please contact your safeguarding children officer for further advice.
	Oral	Warning + 6 months	Confidentially dispose	
	Written – level 1	Warning +6 months	Confidentially dispose	
	Written – level 2	Warning +12 months	Confidentially dispose	
	Final warning	Warning +18 months	Confidentially dispose	
	Dismissal	Termination + 25 years	Confidentially dispose	
	Case not found	Until the person's normal retirement age, or 10 years from the date of the allegation whichever is the longer.	Confidentially dispose	
	Records relating to accident/injury at work	3 years after accident OR 6 years after incident OR 40 years from investigation if serious. In the case of serious accidents a further retention period will need to be applied	Confidentially dispose	
	Maternity pay records	Current year +3	Confidentially dispose	
	Records held under Retirement Benefits Schemes (Information	Current year + 6	Confidentially dispose	

	Powers) Regulations 1995			
	Proofs of identity collected as part of the process of checking "portable" enhanced CRB disclosure	Add to personnel file	Confidentially dispose	
Child protection	Child Protection files	From deregistration + 25 years	Confidentially dispose	Child Protection information must be copied and sent under separate cover to new school/college whilst the child is still under 18 (i.e. the information does not need to be sent to a university for example). Where a child is removed from roll to be educated at home, the file should be copied to the Local Education Authority.

	Allegation of a child protection nature against a member of staff, including where the allegation is unfounded	Until the person's normal retirement age, or 10 years from the date of the allegation whichever is the longer	Confidentially dispose	The following is an extract from "Safeguarding Children and Safer Recruitment in Education" p60 "Record Keeping 5.10 It is important that a clear and comprehensive summary of any allegations made, details of how the allegation was followed up and resolved, and a note of any action taken and decisions reached, is kept on a person's confidential personnel file, and a copy provided to the person concerned. The purpose of the record is to enable accurate information to be given in response to any future request for a reference if the person has moved on. It will provide clarification in cases where a future CRB Disclosure reveals information from the police about an allegation that did not result in a criminal conviction. And it will help to prevent unnecessary reinvestigation if, as sometimes happens, an allegation re-surfaces after a period of time. The record should be retained at least until the person has reached normal retirement age or for a period of 10 years from the date of the allegation if that is longer."
Governing Body	Curriculum complaints records,	Date of resolution of complaint + 6 years	Confidentially dispose	
	Trust endowment papers.	Permanent	Retain in school whilst operationally required then Transfer to Archives	
	Minutes			

	Principal set (signed)	Permanent	Retain in school for 6 years from date of meeting then Transfer to Archives	
	Inspection copies	Date of meeting + 3 years	Confidentially dispose	
	Agendas	Date of meeting	Confidentially dispose	
	Reports	Date of report + 10 years	Transfer to Archives. The archivist will take a sample for permanent preservation.	
	Annual Parents' meeting papers	Date of meeting + 6 years	Transfer to Archives. The archivist will take a sample for permanent preservation.	
	Instruments of Government	Permanent	Transfer to Archives when the school has closed	
	Trusts and Endowments	Permanent	Retain in school whilst operationally required then Transfer to Archives	

	OFSTED Action Plans	Date of action plan + 3 years	Transfer to Archives	
	Policy documents			
	Statutory	Retain statutory policy for a 6 year retention period.		
	Non - Statutory	Expiry of policy	Retain in school whilst policy is operational, then confidentially dispose	
	Complaints files	Date of resolution of complaint + 6 years. Retain in the school for the first 6 years. Review for further retention in the case of contentious disputes. Dispose of routine complaints.	Confidentially dispose	
	Annual Reports required by the Department for Education and Skills	Date of report + 10 years	Transfer to Archives. The archivist will take a sample for permanent preservation.	
	Proposals for schools to become, or be established as Specialist Status schools	Current year + 3 years	Transfer to Archives. The archivist will take a sample for permanent preservation.	
Health and safety:	Health and Safety Inspection (Surveillance) records	Date of incident + 40 years	Confidentially dispose	

	Safety incident reports			
	Adults –	6 years after incident OR 40 years from investigation if serious. In the case of serious accidents a further retention period will need to be applied	Confidentially dispose	
	Child	Retain for 6 years after incident OR until 21 years old, whichever is appropriate OR retain for 40 years from investigation if serious	Confidentially dispose	
	Most other records			
	Accessibility Plans	Current year + 6 years	Confidentially dispose	
	Accident/Incident Reporting			
	Adults	6 years after incident OR 40 years from investigation if serious. In the case of serious accidents a further retention period will need to be applied	Confidentially dispose	
	Children	Retain for 6 years after incident OR until 25 years old, whichever is appropriate OR retain for 40 years from investigation if serious	Confidentially dispose	A child may make a claim for negligence for 7 years from their 18th birthday. To ensure that all records are kept until the pupil reaches the age of 25 this retention period has been applied.
	COSHH	Current year + 10 years [where appropriate an additional retention period may be allocated]	Confidentially dispose	
	Risk Assessments	From risk assessment + 3 years (40 years in some instances). 40 years if record relates to inspection and test of physical and environmental hazards	Confidentially dispose	

	Process of monitoring of areas where employees and persons are likely to have become in contact with asbestos	Last action + 40 years	Confidentially dispose	
	Process of monitoring of areas where employees and persons are likely to have come in contact with radiation	Last action + 50 years	Confidentially dispose	
	Fire Precautions log books	Last entry + 6 years	Dispose	
School organisation records	Visitors book	CY+ 5 years	Transfer to the Archives	
Pupil records:	**Pupils assessment data and electronic information**			
	Admission Registers	Last entry + 3 years	Transfer to the Archives	
	Attendance registers	Last entry + 3 years	Confidentially dispose	Pupil registration is filled out on pre-printed SIMS forms that is scanned into SIMS. The data on SIMS is IDENTICAL to the form. An absence report is printed FROM SIMS and reason for absence can be marked, such as late. This is then scanned INTO SIMS and stored data amended. SIMS for Primary, BROMCOM for Secondary. BROMCOMdata is locally stored and transferred automatically into SIMS, then server backed up.
	Pupil record cards			

	Primary	Retain for the time which the pupil remains at the primary school	Transfer to the secondary school (or other primary school) when the child leaves the school. In the case of exclusion it may be appropriate to transfer the record to the Behaviour Service	
	Secondary	DOB of the pupil +25 years	Confidentially dispose	
	Pupil files			
	Primary	Retain for the time which the pupil remains at the primary school	Transfer to the secondary school (or other primary school) when the child leaves the school.	In the case of exclusion it may be appropriate to transfer the record to the Behaviour Service
	Secondary	DOB of the pupil +25 years	Confidentially dispose	

	Special Educational Needs files, reviews and Individual Education Plans	DOB of pupil + 30 years.	Confidentially dispose	This retention period is the minimum period that any pupil file should be kept. Some authorities choose to keep SEN files for a longer period of time to defend themselves in a "failure to provide a sufficient education" case. There is an element of business risk analysis involved in any decision to keep the records longer than the minimum retention period.
	SEN General	DOB of pupil + 30 years.	Confidentially dispose	For the interagency records there would be a multi-disciplinary meeting and recordings re various pupils with SEN. SEN General category that could be searched against for the particular school and information regarding a specific pupil then identified. If we receive a request for SEN records it is likely to be related to a failure to education claim so we would be prepared for an officer to search under this category also.
	Letters authorising absence	Date of absence + 2 years	Confidentially dispose	
	Absence books	Current year + 6 years	Confidentially dispose	Pupil registration is filled out on pre-printed SIMS forms that is scanned into SIMS. The data on SIMS is IDENTICAL to the form. An absence report is printed FROM SIMS and reason for absence can be marked, such as late. This is then scanned INTO SIMS and stored data amended. SIMS for Primary, BROMCOM for Secondary. BROMCOMdata is locally stored and transferred automatically into SIMS, then server backed up.
	Examination results			

	Public	Year of examinations + 6 years	Confidentially dispose	Any certificates left unclaimed should be returned to the appropriate Examination Board. Exam results are logged therefore no need to keep the actual papers
	Internal examination results	Current year + 5 years	Confidentially dispose	If these records are retained on the pupil file or in their National Record of Achievement they need only be kept for as long as operationally necessary.
	Any other records created in the course of contact with pupils	Current year + 3 years	Review at the end of 3 years and either allocate a further retention period or dispose	
	Statement maintained under The Education Act 1996 - Section 324	DOB + 30 years	Confidentially dispose unless legal action is pending	
	Proposed statement or amended statement	DOB + 30 years	Confidentially dispose unless legal action is pending	
	Advice and information to parents regarding educational needs	Closure + 12 years	Confidentially dispose unless legal action is pending	
	Accessibility Strategy	Closure + 12 years	Confidentially dispose unless legal action is	

			pending	
	Children's SEN Files	DOB of pupil + 25 years then review – it may be appropriate to add an additional retention period in certain cases	Confidentially dispose unless legal action is pending	
	Parental permission slips for school trips – where there has been no major incident	Conclusion of the trip + 3 years	Confidentially dispose	
	Parental permission slips for school trips – where there has been a major incident	DOB of the pupil involved in the incident + 25 years	Confidentially dispose	The permission slips for all pupils on the trip need to be retained to show that the rules had been followed for all pupils
	Records created by schools to obtain approval to run an Educational Visit outside the Classroom - Primary Schools	Date of Visit + 14 years	Confidentially dispose	
	Records created by schools to obtain approval to run an Educational Visit outside the Classroom - Secondary Schools	Date of visit + 10 years	Confidentially dispose	This retention period has been set in agreement with the Safeguarding Children's Officer
	Walking Bus registers	Date of register + 3 years - This takes into account the fact that if there is an incident requiring an accident report the register will be submitted with the accident report and kept for the period of time required for accident reporting	Confidentially dispose	If these records are retained electronically any back up copies should be destroyed at the same time

Materials relating to teaching and the curriculum	***Curriculum records:***			
	Curriculum development	Current year + 6 years	Dispose	
	Curriculum returns	Current year + 3 years	Dispose	
	School syllabus	Current year + 1 then review	It may be appropriate to review these records at the end of each year and allocate a new retention period or Dispose	
	Schemes of work	Current year + 1 then review	It may be appropriate to review these records at the end of each year and allocate a new retention period or Dispose	
	Timetable	Current year + 1 then review	It may be appropriate to review these records at the end of each year and allocate a new	

			retention period or Dispose	
	Class record books	Current year + 1 then review	It may be appropriate to review these records at the end of each year and allocate a new retention period or Confidentially Dispose	
	Mark Books	Current year + 1 then review	It may be appropriate to review these records at the end of each year and allocate a new retention period or Confidentially Dispose	
	Record of homework set	Current year + 1 then review	It may be appropriate to review these records at the end of each year and allocate a new retention	

			period or Dispose	
	Pupils' work	Current year + 1 then review	It may be appropriate to review these records at the end of each year and allocate a new retention period or Confidentially Dispose	
	Examination results	Current year + 6 years	Confidentially dispose	
	SATS records	Current year + 6 years	Confidentially dispose	
	PANDA reports	Current year + 6 years	Confidentially dispose	
	Value added records	Current year + 6 years	Confidentially dispose	
The schools management information	Professional development plans	Closure + 6 years	Transfer to Archives	
	School development plans	Closure + 6 years	Transfer to Archives	
	Admissions – if the admission is successful	Admission + 1 year	Confidentially dispose	
	Admissions – if the appeal is unsuccessful	Resolution of case + 2 year	Confidentially dispose	

	Admissions – Secondary Schools – Casual	Current year + 1 year	Confidentially dispose	
	Proofs of address supplied by parents as part of the admissions process	Current year + 1 year	Confidentially dispose	
	Employer's Liability certificate	Closure of the school + 40 years	Dispose	
	School brochure or prospectus	Current year + 3 years	Transfer to Archives	
	Circulars (staff/parents/pupils)	Current year + 1 year	Dispose	
	Newsletters, ephemera	Current year + 1 year	Transfer to Archives	
	PTA/Old Pupils Associations	Current year + 6 years	Transfer to Archives	
Finance records	Annual Accounts	Current financial year + 6 years	Transfer to Archives	
	Loans and grants	Date of last payment on loan + 12 years	Review to see whether a further retention period is required then transfer to Archives	
	Contracts			
	under seal	Contract completion date + 12 years	Confidentially dispose	
	under signature	Contract completion date + 6 years	Confidentially dispose	
	Monitoring records	Current financial year + 2 years	Confidentially dispose	

	Copy orders	Current financial year + 2 years	Confidentially dispose	
	Budget reports, budget monitoring etc	Current financial year + 3 years	Confidentially dispose	
	Invoice, receipts and other records covered by the Financial Regulations	Current financial year + 6 years	Confidentially dispose	
	Teacher's payment invoices e.g. additional hours payment for break duty etc.	Current financial year + 6 years	Confidentially dispose	
	Annual Budget and background papers	Current financial year + 6 years	Confidentially dispose	
	Order books and requisitions	Current financial year + 6 years	Confidentially dispose	
	Delivery Documentation	Current financial year + 6 years	Confidentially dispose	
	Debtors' Records	From time of last action+ 6 years	Confidentially dispose	
	Cheque books	Current financial year + 3 years	Confidentially dispose	
	Paying in books	Current financial year + 6 years then review	Confidentially dispose	
	Ledger	Current financial year + 6 years then review	Confidentially dispose	
	Invoices	Current financial year + 6 years then review; Copies current financial year + 3	Confidentially dispose	
	Receipts	Current financial year + 6 years	Confidentially dispose	
	Bank statements	Current year + 6 financial years then review	Confidentially dispose	
	School Journey books	Current year + 6 financial years then review	Confidentially dispose	
	Applications for free school meals, travel,	Whilst child at school	Confidentially dispose	

	uniforms etc			
	Student grant applications	Current year + 3 financial years	Confidentially dispose	
	Free school meals registers	Current year + 6 financial years	Confidentially dispose	
	Petty cash books	Current year + 6 financial years	Confidentially dispose	
Property records	Title Deeds	Until interest in property ceases	These should follow the property unless the property has been registered at the Land Registry. Transfer to Archives if the deeds are no longer needed	
	Plans	Permanent	Retain in school whilst operational then Transfer to Archives	
	Maintenance and contractors	Current year + 6 years	Confidentially dispose	
	Leases	Expiry of lease + 6 years	Confidentially dispose	LA keeps a copy of these, but if a school issues on their own should be kept for the retention period
	Lettings	Current year + 3 years	Confidentially dispose	Only need keeping as proof of a revenue stream
	Burglary, theft and vandalism report forms	Current year + 6 years	Confidentially dispose	

	Maintenance log books	Last entry + 10 years	Dispose	
	Contractors' Reports	Current year + 6 years	Confidentially dispose	
All other important and prime documentation	Child Protection files	DOB + 25 years	Confidentially dispose	Child Protection information must be copied and sent under separate cover to new school/college whilst the child is still under 18 (i.e. the information does not need to be sent to a university for example). Where a child is removed from roll to be educated at home, the file should be copied to the Local Education Authority.
	Allegation of a child protection nature against a member of staff, including where the allegation is unfounded	Until the person's normal retirement age, or 10 years from the date of the allegation whichever is the longer	Confidentially dispose	It is important that a clear and comprehensive summary of any allegations made, details of how the allegation was followed up and resolved, and a note of any action taken and decisions reached, is kept on a person's confidential personnel file, and a copy provided to the person concerned. The purpose of the record is to enable accurate information to be given in response to any future request for a reference if the person has moved on. It will provide clarification in cases where a future CRB Disclosure reveals information from the police about an allegation that did not result in a criminal conviction. And it will help to prevent unnecessary reinvestigation if, as sometimes happens, an allegation re-surfaces after a period of time. The record should be retained at least until the person has reached normal retirement age or for a period of 10 years from the date of the allegation if that is longer."

	Secondary transfer sheets (Primary)	Current year + 2 years	Confidentially dispose	
	Attendance returns	CY+ 1 year	Confidentially dispose	
	Circulars from LEA	Whilst required operationally	Confidentially dispose	
	HMI reports	These do not need to be kept any longer	Transfer to Archives	
	OFSTED reports and papers	Replace former report with any new report	Transfer to Archives	
	Returns	Current year + 6 Years	Confidentially dispose	
	Circulars from Department for Children, Schools and Families	Whilst operationally required	Transfer to Archives	
	Connexions:			
	Service level agreements	Until superseded	Dispose	
	Work Experience agreement	DOB of child + 18 years	Confidentially dispose	
	School meals:			
	Dinner Register	completion + 3 years	Dispose	
	School Meals Summary Sheets	completion + 3 years	Dispose	
	Family liaison officers and parent support assistants:			
	Day Books	Current year + 2 years then review	Confidentially dispose	

	Reports for outside agencies – where the report has been included on the case file created by the outside agency	Whilst child at school then destroy	Confidentially dispose	
	Referral forms	While the referral is current then destroy	Confidentially dispose	
	Contact data sheets	Current year then destroy if contact no longer active	Confidentially dispose	
	Contact database entries	Current year then destroy if contact no longer active	Confidentially dispose	
	Group Registers	Current year + 2 years	Confidentially dispose	
	Early Years provision – records to be kept by all registered persons – all cases:			
	The name, home address and date of birth of each child who is looked after on the premises	Closure of setting + 50 years	Confidentially dispose	These could be required to show whether or not an individual child attended the setting in a child protection investigation]. If this information is kept in the same book or on the same form as above then the same retention period should be used. If the information is stored separately, then destroy once the child has left the setting (unless the information is collected for anything other than emergency contact).
	The name, address and telephone number of any person who will be looking after children on the premises	Termination of employment + 6 years then review	Confidentially dispose	

	A daily record of the names of children looked after on the premises, their hours of attendance and the names of the persons who looked after them	End of academic year + 2 years	Confidentially dispose	If these records are likely to be needed in a child protection setting then the records should be retained for closure of setting + 50 years
	A record of accidents occurring on the premises and incident books relating to other incidents	See above	Confidentially dispose	
	A record of any medicinal product administered to any child on the premises, including the date and circumstances of its administration, by whom it was administered, including medicinal products which the child is permitted to administer to himself, together with a record of parent's consent	DOB of the child being given/taking the medicine + 25 years	Confidentially dispose	
	Records of transfer	One copy is to be given to the parents, one copy transferred to the Primary School where the child is going	Confidentially dispose	
	Portfolio of work, observations and so on	To be sent home with the child	N/A	

	Birth certificates	Once the setting has had sight of the birth certificate and recorded the necessary information the original can be returned to the parents. There is no requirement to keep a copy of the birth certificate.	N/A	
	Records to be kept by Registered Persons - Day Care:			
	A statement of the procedure to be followed where a parent has a complaint about the service being provided by the registered person	Until superseded	Confidentially dispose	
	A statement of the arrangements in place for the protection of children, including arrangements to safeguard the children from abuse or neglect and procedures to be followed in the event of allegations of abuse or neglect	Closure of setting + 50 years	Confidentially dispose	These could be required to show whether or not an individual child attended the setting in a child protection investigation.
	Other records - administration:			
	Financial Records			
	Financial records – accounts, statements, invoices, petty cash etc	Financial year + 6 years	Confidentially dispose	

	Insurance			
	Insurance policies – Employers Liability	Life of policy + 40 years	Dispose	
	Claims made against insurance policies – damage to property	Settlement of claim + 6 years	Confidentially dispose	
	Claims made against insurance policies – personal injury	6 years or 6 years from 18th birthday whichever is later.	Confidentially dispose	
	Human Resources			
	Personal Files - records relating to an individual's employment history	Termination + 25 years	Confidentially dispose	
	Pre-employment vetting information (including CRB checks)	Keep for maximum of six months following the recruitment decision unless a dispute is raised or, in exceptional circumstances, where CRB agreement is secured	Confidentially dispose	
	Staff training records – general	Current year + 2 years	Confidentially dispose	
	Training (proof of completion such as certificates, awards, exam results)	Last action + 7 years	Confidentially dispose	
	Premises and Health and Safety			
	Premises files (relating to maintenance)	Cessation of use of building + 7 years then review	Dispose	
	Risk Assessments	6 years (40 years in some instance) from elimination of risk/updating of Risk Assessment	Confidentially dispose	
Other documents from the RM Guidance	Proposals for schools to become, or be established as Specialist Status	Current year + 3 years	Transfer to Archives	

	schools			
	Log Books	Date of last entry in the book + 6 years	Retain in school for 6 years from last entry then Transfer to Archives	
	Minutes of the Senior Management Team and other internal administrative bodies	Date of meeting + 5 years	Transfer to Archives	
	Reports made by the head teacher or the management team	Date of report + 6 years	Transfer to Archives	
	Records created by head teachers, deputy heads, heads of year and other members of staff with administrative responsibilities.	Closure of file + 6 years	Confidentially dispose	
	Correspondence created by head teachers, deputy heads, heads of year and other members of staff with administrative responsibilities.	Date of report + 3 years	Confidentially dispose	
	Annual appraisal/assessment records	Current year + 5 years	Confidentially dispose	
	Inventories of equipment and furniture	Current year + 6 years	Dispose	

	General file series	Current year + 5 years	Transfer to Archives	
	The name and address and telephone number of the registered person and every other person living or employed on the premises.	Termination + 6 years then review	Confidentially dispose	
	A statement of the procedure to be followed in the event of a fire or accident	Procedure superseded + 7 years	Dispose	
	A statement of the procedure to be followed in the event of a child being lost or not collected	Procedure superseded + 7 years	Dispose	

Appendix 4

Information Sharing Checklists
(Adapted from Guidance issued by the ICO)

These two checklists provide a reference guide to support the decision making process of whether to share personal information. The checklists should be used alongside guidance provided in the ICO Data Protection Code of Practice and highlight relevant considerations to ensure the sharing complies with the law and meets individuals' expectations.

Information Sharing Checklist: Systematic Information Sharing

Scenario: Entering into an agreement to share personal information on an ongoing basis.

Is the sharing justified?

- What is the sharing meant to achieve?
- Have you assessed the potential benefits and risks to individuals and/or society of sharing or not sharing?
- Is the sharing proportionate to the issue you are addressing?
- Could the objective be achieved without sharing the personal information?

Do you have the power to share?

Key points to consider:

- The type of organisation you work for and any relevant functions or powers of your organisation.
- The nature of the information you have been asked to share (for example, was it given in confidence?)
- Any legal obligation to share information (for example a statutory requirement or court order).

If you decide to share:

It is good practice to have an information sharing agreement in place. As well as considering the key points above, your information sharing agreement should cover the following issues:

- What information needs to be shared
- The organisations that will be involved.
- What you need to tell people about the information sharing and how you communicate that information.
- Measures to ensure adequate security is in place to provide individuals with access to their personal information if they request it.
- Agreed, common retention periods for the information and processes are in place to ensure deletion takes place.

Appendix 5

Information Sharing Checklists
(*Adapted from Guidance issued by the ICO)*

These two checklists provide a reference guide to support the decision making process of whether to share personal information. The checklists should be used alongside guidance provided in the ICO Data Protection Code of Practice and highlight relevant considerations to ensure the sharing complies with the law and meets individuals' expectations.

Information Sharing Checklists: One Off Requests

Scenario: You are asked to share personal information relating to an individual in "one off" circumstances.

Is the sharing justified?

Key points to consider:

- Do you think you should share the information?
- Have you assesses the potential benefits and risks to individuals and/or society of not sharing?
- Do you have concerns that an individual is at risk of serious harm?
- Do you need to consider an exemption in the DPA to share?

Do you have the power to share?

Key points to consider:

- The type of organisation you work for.
- Any relevant functions or powers of your organisation.
- The nature of the information you have been asked to share (for example, was it given in confidence?)
- Any legal obligation to share information (for example, a statutory requirement or a court order).

If you decided to share:

Key points to consider:

- What information do you need to share?
- Only share what is necessary.
- Distinguish fact from fiction.
- How should the information be shared?
- Information must be shared securely.
- Ensure you are giving the information to the right person.
- Consider whether it is appropriate/safe to inform the individual that you have shared their information.
- Record your information sharing decision and your reasoning – whether you shared the information or not.

If you share the information you should record:

- What information was shared and for what purpose.
- Who was it shared with.
- When was it shared.
- Your justification for sharing.
- Whether the information was shared with or without consent.

Appendix 6

Specimen Recording a Request to Share Information Form.
(Adapted from guidance from the ICO)

Name of organisation	
Name of person requesting information:	
Job title of person requesting information	
Date of request	
Purpose	
Date required by	
Specific arrangement related to transfer of information:	
Specific arrangement related to retention/deletion of data	
Signed	
Dated	

Appendix 7

Specimen Recording a Decision to Share Information Form.
(Adapted from guidance from the ICO)

Name of organisation	
Name of person requesting information:	
Job title of person requesting information	
Date request received	
Date requested	
Purpose	
Decision	
Decision taken by: **Name:** **Job Title:**	
Date supplied	
Reason for disclosure/non disclosure	
Specific arrangement related to transfer of	

information:	
Specific arrangement related to retention/deletion of information	
Date of disclosure	
Signed	
Dated	

Appendix 8

Specimen Information Sharing Agreement

In order to adopt good practice and to comply with the DPA, the ICO would expect an information sharing agreement to address the following issues:

Specimen Information Sharing Agreement

Purpose of the information sharing initiative: *(Your agreement should explain why the information sharing is necessary, the specific aims you have and the benefits you expect to bring to individuals or society more widely. This should be precise so that all parties are absolutely clear about the purposes for which information may be shared and the shared information used.)*
The organisations that will be involved in the information sharing: *(Your agreement should clearly identify all the organisations that will be involved in the information sharing and should include contact details for key members of staff and ICO Registration Number. It should also contain procedures for including additional organisations as required and removing organisations if necessary.)*
Information to be shared: *(This section should detail the types of information to be shared with the organisations stated above. This may need to be quite detailed because in some cases it will be appropriate to share certain details held in a files about someone, but not other more sensitive information. In some cases it may be appropriate to attach "permissions" to certain items so that only certain members of staff that have received appropriate access are given access access to them.)*
Basis for sharing: *(The basis for sharing needs to be clear. If you are a public sector body you may be under a legal duty to share certain types of personal information. Even if you are not under a legal requirement to share information you should explain*

if you have the legal power which allows you to share. You should explain how the disclosures will be consistent with the DPA. If consent is to be a basis for disclosure your agreement should contain a model consent form. It should also address issues surrounding the withholding or retraction of consent.)

Access and Individuals' Rights:

(The agreement should explain what to do when an organisation receives a Subject Access or Freedom of Information request. In particular, it should ensure that one staff member or organisation takes overall responsibility for ensuring that the individual can gain access to all the shared information easily. Although decisions about access will often have to be taken on a case by case basis, your agreement should give a broad outline of the sorts of informational you will normally release in response to either Subject Access or Freedom of Information requests. It should also address the inclusion of certain types of information in your publication scheme.

Information Governance:

- *(Your agreement should deal with the main practical problems that may arise when sharing personal information. This should ensure that all organisations involved in the sharing:*
- *have detailed advice about which information may be shared to prevent irrelevant or excessive information being disclosed,*
- *make sure that information being shared is accurate, for example by periodic sampling or audit,*
- *are using compatible datasets and are recording information in the same way,.*
- *have common rules for the retention and deletion of shared information and procedures for dealing with cases where different organisations may have different statutory or professional retention or deletion rules,*
- *have common technical and organisational security arrangements, including for the transmission of the information and procedures for dealing with any breach of the agreement,*
- *have procedures for dealing with Subject Access or Freedom of Information requests or other complaints and queries from members of the public,*
- *have a timescale for assessing the ongoing effectiveness of the sharing*

initiative and the agreement that governs it, and

- *have procedures for dealing with the termination of the information sharing agreement, including the deletion of the share data or its return to the organisation that supplied it originally.)*

Appendices:

You may want to include:

- *A glossary of key terms*
- *A summary of the key legislative provisions, for examples relevant sections of the DPA or reference to any legislation that provides your legal basis for sharing information.*
- *A pro forma for seeking individuals' consent for information sharing, and*
- *A diagram to show how to decide whether to share information, an information sharing request form and an information sharing decision form.*

Appendix 9

Information Security Checklist for Schools

	Yes	No	Pending	Action Required	Responsible	Review Date
1. Is the school registered as a Data Controller with the Information Commissioner's Office?						
2. Does the school have a structure in place to effective monitor and evaluate processes, procedures and training to ensure safe and secure handling of information in line with DPA?						
3. Does the school have an up to date Privacy Notice and effective methods of communicating it to pupils, families, staff and others?						
4. Does the school have an Information Security Policy that is reviewed annually?						
5. Does the school have an Acceptable Use Policy for Staff that is reviewed annually?						
6. Does the school Data Protection Policy include a requirement to immediately notify the Land the ICO of data breaches?						
7. Is the school's electronic information backed up?						
8. Is the method of backup secure?						

	Yes	No	Pending	Action Required	Responsible	Review Date
9. How often is it backed up and what is the maximum age of the backup?						
10. If information is held in cloud storage does it meet DPA requirements?						
11. Are servers holding personal information in a locked room or cabinet with restricted access?						
12. Are servers protected from environmental damage?						
13. Are users who access personal information required to have a unique username and strong/complex password?						
14. Are password changes forced – at least once a term?						
15. Are the users and network account which have access to personal information reviewed (at least annually) and kept current?						
16. Is the access to personal information restricted to those who need the information to do their job?						
17. Is there a process for reviewing access/deleting accounts for staff changing roles/leavers?						

	Yes	No	Pending	Action Required	Responsible	Review Date
18. Do the devices used by staff that access personal information have a password protected inactivity activated screensaver or lock out?						
19. Are screens located to ensure they cannot be overlooked?						
20. Is remote access to personal information from outside the school controlled, limited, password protected and conducted over an encrypted channel?						
21. Are portable devices (such as laptops) secured (for example by Kensington lock) when in use?						
22. Are portable devices (such as laptops) encrypted and password protected?						
23. Does the school have processes to manage the use of removable media (USBs), who uses it and for what and is it encrypted?						
24. Are paper records held securely in locked cabinets within restricted access?						
25. Does the school have a method for secure disposal of paper records?						
26. Does the school have processes for retrieving all computer equipment and removable media from leavers?						

	Yes	No	Pending	Action Required	Responsible	Review Date
27. Does the school have processes for secure disposal of redundant IT equipment and removal media and tracking the disposal?						
28. Does the school website have controls in place to prevent unauthorised access including to restricted information?						
29. Is the school website compliant with DPA requirements including the use of "Cookies "and similar technologies?						
30. Does the school have a process for regularly reviewing the security of the building to enforce restricted access and unauthorised access?						
31. Are school staff aware of the processes for ensuring information security and are they trained to meet their requirements?						
32. Are schools aware of who they can share information with and how they should do it securely?						
33. Are information sharing agreements in place as required?						
35. Does the school use third parties to process data for them? Is a data processing agreement in place?						
32. Does the school have a process for recording and responding to Subject Access and Freedom of Information requests?						