SAINTS PETER AND PAUL
CATHOLIC HIGH SCHOOL

Information Security Policy

Last updated: April 2017

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.

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 THIS POLICY

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 persons 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, students, suppliers, clients and others. This personal information must be dealt with lawfully, correctly and in compliance with the DPA.

3.0 ROLE OF THE INFORMATION COMMISSIONERS OFFICE

The role of the Information Commissioner and their 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 INFORMATION COMMISSIONERS OFFICE REQUIREMENTS

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.

This policy outlines the Saints Peter and Paul Catholic high school response to these requirements.

4.0 DEFINITION OF INFORMATION AND 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 and Saints Peter and Paul Catholic high school will ensure that:

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 1) is met, and
B. in the case of sensitive personal information, at least one of the conditions in Schedule 3 (Appendix 1) 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 Notification: Saints Peter and Paul Catholic high school will register annually with the ICO as notification that we are processing personal information.

5.2 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. Saints Peter and Paul Catholic high school will publish a privacy notice on correspondence and website. This notice will also reference the use of CCTV in the school premises.

5.3 Subject Access and Freedom of Information Requests: These requests will be processed in line with the Saints Peter and Paul Catholic high school Freedom of Information Policy.

6.0 INFORMATION THAT NEEDS TO BE PROTECTED

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).

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 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. The Principal has ultimate responsibility as data controller and needs to be supported in this by an information governance structure with clear lines of responsibility. This governance structure is 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):

Saints Peter and Paul Catholic high school will designate staff who are responsible for working out exactly what information needs to be secured and the measures in place to do so. 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.

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
- Ensure 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.

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 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
- Recognising potential or actual information security incidents, initiating reporting and
- Actioning mitigation 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 students, staff, families and so on).

Saints Peter and Paul Catholic high school will 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 will ensure that the IAR is reviewed, updated and maintained. It is a critical document that will be included in the school business continuity plan.

7.2 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. Providing 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 the information they need, that the information is valued and that it is protected.

7.3 Organisational Measures to Protect Information

An information and data security audit will take place annually to ensure that Saints Peter and Paul Catholic high school protect information and risk assess the controls that are in place. Systems and procedures will be put in place 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 will 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. Record retention schedule is included in appendix 2.

7.3.2 Protective Markings: Saints Peter and Paul Catholic high school will 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. Saints Peter and Paul Catholic high school will implement a complex password process which supports improved security on devices accessing the school 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 online accounts or saved in web browsers. Passwords must never be emailed to someone else.

7.3.4 Device hardening: Saints Peter and Paul Catholic high school takes great care to protect the school network against malicious virus attacks and the importance of having the right technical support in place cannot be underestimated. Computers need regular updates to their operating systems, web browsers and security software (antivirus and antispyware).

Devices connecting to the school network will have to 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.

7.3.5 Email: Staff are provided with an approved email address in the format of

"@saintspeterandpaul.halton.sch.uk"

Non-approved email accounts must not be used to conduct official business. All emails that represent aspects of official business are the property of the business and not the individual.

7.3.6 Websites: The website provides an essential marketing and information tool. Important considerations include:

- Disclosure of personal information – including images – without consent.

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

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

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. Saints Peter and Paul Catholic high school will comply with this guidance.

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 will 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 safeguarding implications may apply.

If Saints Peter and Paul Catholic high school wants to record an activity to sell on to families, we will ensure that we are complying with the DPA.

7.3.9 Social Networking: Saints Peter and Paul School has an ESafety/Acceptable Use Policy and Staff Code of Conduct which outlines expectations in relation to the use of social networking. 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).

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.

At Saints Peter and Paul Catholic high school employees 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. An unencrypted device is a security risk.

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”.

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 prior to entering into a contract, that a thorough risk assessment is undertaken.

7.4 Security of Mobile Technologies:

7.4.1 Laptops: 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 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 screen lock
- 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 (Ctrl, Alt, Del) when unattended
- be protected with approved encryption software.

Staff should never:

- leave devices unattended unless security in place
- leave devices unattended in a car unless it is unavoidable and out of sight
- let unauthorised people use their laptop
- use hibernate or standby

Processes will be put 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 will be appropriately wiped 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.

Saints Peter and Paul Catholic high school owned USBs and other removable media will be allocated to staff if required via a semi-permanent loan form. The Principal reserves the right to request return of these devices at any time. Procedures will be established to ensure that these devices are returned at the end of employment. Devices will be appropriately wiped prior to reissue or disposed of securely.

7.4.3 Bring Your Own Device (BYOD): Prior to using personally owned devices in school for business use, staff are required to sign and return the Acceptable Use Agreement. BOYD will be subject to the following controls:

- Devices will be required to have a screen lock which is password protected
- Personal sensitive information will not be downloaded onto unsecure devices
- When accessing emails from BOYDs, passwords should not be set up to be automatically populated.

This security barrier should not be bypassed.

8.0 RETENTION OF INFORMATION

8.1 Retention Periods: The Records Management Retention Schedule (Appendix 2) is followed at Saints Peter and Paul Catholic high school. This document is in line with DPA requirement to keep data for no longer than is necessary.

8.2 Destruction of records: Saints Peter and Paul Catholic high school uses accredited Confidential Waste Bins to destroy any printed or written documents containing personal, confidential and/or sensitive personal information. Under no circumstances will personal, confidential and/or sensitive data be placed in general waste or recycling bins. Crosscut shredders can also be used for the disposal of this type of information.

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.

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. At Saints Peter and Paul Catholic high school 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 off site 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 off site
- 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
- 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. Saints Peter and Paul Catholic high school will include the use of CCTV in their publication scheme. We will also inform staff, students and visitors why personal information is being collected in the form of CCTV images. Careful consideration is 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 and CD) the necessary encryption protocols need to be verified as in place.

Personal sensitive information will not be sent by fax, as this is a particularly vulnerable method of transfer, unless there is no other alternative and to not send the information would cause a serious disruption to service delivery or potentially cause harm. In these circumstances the correct telephone number will be verified by a second employee and confirmed before sending.

If a request is received to transfer printed or written personal, confidential and/or sensitive information, it will be ensured 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 staff is delivering personal information by hand, they will ensure that they verify the identity of who they are handing it to and get a signature.

Saints Peter and Paul Catholic high school will ensure that guidance to staff on whom 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 3 (Systematic Information Sharing) and Appendix 4 (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 5 (Specimen Recording a Request for Information Form) and Appendix 6 (Specimen Recording a Decision to Share Information Form).

Saints Peter and Paull Catholic high school will 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 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 processor 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 Information Sharing Agreements: Information sharing agreements will 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 Saints Peter and Paul Catholic high school collects and shares personal information in compliance with the law, fairly, transparently and in line with the rights of the people whose information is being shared. A specimen information sharing agreement containing key information to be included is attached as Appendix 7 and will be used as the basis of our information sharing agreements.

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 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). 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

Saints Peter and Paul Catholic high school staff will 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. Saints Peter and Paul Catholic high school 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 Freedom of Information: This act gives a right to access information held by public authorities. Under the Act we are required to produce a "publication scheme" which is effectively a guide to the information they hold which is publicly available. Saints Peter and Paul Catholic high school will 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. A record of such requests and responses will be kept.

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 Senior Information Risk Owner will be informed. The response to the incident will include a recovery plan and, where necessary, procedures for damage limitation.
2. **Assessing the risks**: Risks will be assessed in association with the breach, as these are likely to affect what is to be done once the breach has been contained. In particular, Saints Peter and Paul Catholic high school will 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. The SIRO will be clear about who needs to be notified and why. Consideration should be given to notifying the individuals concerned; the ICO; other regulatory bodies; other third parties such as service providers, police and the banks; or the media.
4. **Evaluation and response:** An investigation will take place to establish the causes of the breach and also evaluate the effectiveness of the response to it. If necessary, policies and procedures should be updated accordingly. Near misses should be managed in the same way as a breach.

13.0 MONITORING AND COMPLIANCE

The information governance structure, this policy and linked procedures will be reviewed annually and approved by governors. Robust policies and procedures, training, technical controls and organisational processes will be monitored. Training and awareness rising are critical to creating an organisational culture where information is valued and protected.

14.0 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

15.0 USEFUL LINKS

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

Appendix 1

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;
- 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 2 School Record Retention Schedule Table to be inserted

Appendix 3

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 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 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 5

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 6

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 7

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.*