St Bede's
Catholic School
& Sixth Form College

DATA PROTECTION
POLICIES AND PROCEDURES

Full Governing Body Approval	
Name: Mrs J Leech	Signature:
Date: Autumn Term 18/19	11th October 2018 (FGB)
Review Date: Autumn Term 2020/2021	

A

Data Protection and Information Security and Procedure Policy - General

Introduction

1. Purpose

The purpose of this policy and procedure is to ensure compliance of St. Bede's Catholic School & Sixth Form College with all of its obligations as set out in the Data Protection legislation.

2. Data Controller

The School is the Data Controller as defined in the Data Protection Act 1998.

3. Notification with the Information Commissioner's Office (ICO)

The School notified the ICO, when it was established, using the on-line form http://www.ico.gov.uk/for_organisations/data_protection/notification/notify.aspx

4. Definitions

- **Personal data** is information that relates to an identifiable living individual that is processed as data. Processing means collecting, using, disclosing, retaining, or disposing of information. The data protection principles apply to all information held electronically or in structured files that tells you something about an identifiable living individual. The principles also extend to all information in education records. Examples would be names of staff and pupils, dates of birth, addresses, national insurance numbers, school marks, medical information, exam results, SEN assessments and staff development reviews.
- **Sensitive personal data** is information that relates to race and ethnicity, political opinions, religious beliefs, membership of trade unions, physical or mental health, sexuality and criminal offences. There are greater legal restrictions on processing sensitive personal data than there are on personal data.

5. Data Protection Principles

The eight core principles of the Data Protection Act are enshrined in this policy in the school's commitment that personal data:

- Is processed fairly and lawfully;
- Is obtained only for lawful purposes, and is not further used in any manner incompatible with those original purposes;
- Is accurate and, where necessary, kept up to date;
- Is adequate, relevant and not excessive in relation to the purposes for which it is processed;
- Is not kept for longer than is necessary for those purposes;
- Is processed in accordance with the rights of data subjects under the DPA;
- Is protected by appropriate technical and organisational measures against unauthorised or unlawful processing and against accidental loss, destruction or damage; and
- Is not transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection of the personal information.

6. Fair Processing

The school is committed to being clear and transparent about what type of personal information we hold and how it is used. The following 'Privacy Notice for Pupils and their Parents and Guardians' will be published on the School Website.

7. Privacy Notice for Pupils and their Parents and Guardians

Why do we collect information?

The school collects information about our pupils and holds this personal data so that we can:

- Support each pupil's learning;

- Monitor and report on each pupil's progress;
- Provide appropriate pastoral care and other support to each of our pupils; and
- Assess how well each pupil is doing and report on that to the parents.

What type of information do we collect?

- The information will include: personal data such as name and date of birth as well as contact details; educational performance assessments; attendance information; pastoral information. It will also include sensitive personal data such as: ethnicity; special educational needs; behavioural incidents; and medical information that will help us to support each pupil's education and wider welfare needs at the school.
- We will also hold personal contact information about parents and carers so that we can get hold of you routinely or in an emergency.
- Where CCTV is used by the school this will only be for general security purposes in order to protect the pupils and staff of the school.
- Pupil photographs may be included, as part of their personal data and this will be treated with the same level of confidentiality as all other personal data. Photographic images of pupils used in publically available media such as web sites, newsletters or the school prospectus will not identify pupils unless parental permission has been given in advance.

Do we share this information with anyone else?

We do not share any of this data with any other organisation without your permission except where the law requires it. We are required to provide pupil data to central government through the Department for Education (DfE www.education.gov.uk) and the Education Funding Agency (EFA www.education.gov.uk/efa). Where it is necessary to protect a child, the school will also share data with the Local Authority Children's Social Services and/or the Police.

Can we see the personal data that you hold about our child?

All pupils have a right to have a copy of the personal information held about them. As our pupils are of secondary school age, a request for a copy of the personal information has to be made by a parent or guardian in writing. The only circumstances under which the information would be withheld would be if there was a child protection risk, specifically:

  - The information might cause serious harm to the physical or mental health of the pupil or another individual;
  - Where disclosure would reveal a child is at risk of abuse;
  - Information contained in adoption or parental order records;
  - Information given to a court in proceedings under the Magistrate's Courts (Children and Young Persons) Rules 1992; and
- Copies of examination scripts.
- If you want a printed copy of the personal data then the school will charge the actual cost of providing the copy up to a maximum of a £10 charge. To protect each child's right of confidentiality under law the school reserves the right to check the identity of a person making a request for information on a child's behalf. Once any identity check has been completed and any fee due paid, the information will be collected and provided within 40 calendar days.

Can we see our child's educational record?

- All parents are also entitled to a copy of their child's educational record. A request must be made in writing to the Governing Body. The Educational Record includes curriculum, assessment, pastoral and behavioural information that is stored by the school. Only

information that has come from a teacher or employee of the school can be considered to form part of the educational record.

- The school will charge a fee to provide an actual copy of the educational record but this will not be greater than the actual cost of reproducing the information. Once any fee has been received the school will respond to the request within 15 school days (21 calendar days excluding any public or school holidays).

8. Information Security

Objective

The information security objective is to ensure that the school's information base is protected against identified risks so that it may continue to deliver its services and obligations to the community. It also seeks to ensure that any security incidents have a minimal effect on its business and academic operations.

Responsibilities

The Headteacher of the school has direct responsibility for maintaining the Information Security policy and for ensuring that the staff of the school adheres to it.

General Security

It is important that unauthorised people are not permitted access to school information and that we protect against theft of both equipment and information. This means that we must pay attention to protecting our buildings against unauthorised access. Staff must:

- Not reveal pin numbers or building entry codes to people that you do not know or who cannot prove themselves to be employees;
- Beware of people tailgating you into the building or through a security door;
- If you don't know who someone is and they are not wearing some form of identification, ask them why they are in the building;
- Not position screens on reception desks where members of the public could see them;
- Lock secure areas when you are not in the office;
- Not let anyone remove equipment or records unless you are certain who they are;
- Visitors and contractors in school buildings should always sign in to the visitor's book.

Security of Paper Records

- Paper documents should always be filed with care in the correct files and placed in the correct place in the storage facility.
- Records that contain personal data, particularly if the information is sensitive should be locked away when not in use and should not be left open or on desks overnight or when you are not in the office;
- Always keep track of files and who has them;
- Do not leave files out where others may find them;
- Where a file contains confidential or sensitive information, do not give it to someone else to look after.

Security of Electronic Data

Most of our data and information is collected, processed, stored, analysed and reported electronically. It is essential that our systems, hardware, software and data files are kept secure from damage and unauthorised access. School staff must:

- Prevent access to unauthorised people and to those who don't know how to use an item of software properly. It could result in loss of information;

- Keep suppliers CDs containing software safe and locked away. Always label the CDs so you do not lose them in case they need to be re-loaded;
- When we buy a license for software, it usually only covers a certain number of machines. Make sure that you do not exceed this number, as you will be breaking the terms of the contract.
- Passwords are a critical element of electronic information security. All staff must manage their passwords in a responsible fashion:
    - Don't write it down;
    - Don't give anyone your password;
    - Your password should be at least 6 characters;
    - The essential rules your password is something that you can remember but not anything obvious (such as password) or anything that people could guess easily such as your name;
- You can be held responsible for any malicious acts by anyone to whom you have given your password;
- Include numbers as well as uppercase letters in the password;
- Take care that no-one can see you type in your password;
- Change your password regularly, and certainly when prompted. Also change it if you think that someone may know what it is.
- Many database systems, particularly those containing personal data should only allow a level of access appropriate to each staff member. The level may change over time.

Use of E-Mail and Internet

- The use of the school's e-mail system and wider Internet use is for the professional work of the school. Reasonable personal use of the system in a member of staff's own time is permitted but professional standards of conduct and compliance with the school's wider policies are a requirement whenever the e-mail or Internet system is being used. The school uses a filtered and monitored broadband service to protect our pupils. Deliberate attempts to access web sites that contain unlawful, pornographic, offensive or gambling content are strictly prohibited. Staff discovering such sites on the system must report this to the Director of ICT Services immediately.
- To avoid a computer virus arriving over the Internet, do not open any flashing boxes or visit personal websites;
- Do not send highly confidential or sensitive personal information via e-mail;
- Save important e-mails straight away;
- Unimportant e-mails should be deleted straight away;
- Do not send information by e-mail, which breaches the Data Protection Act. Do not write anything in an e-mail which could be considered inaccurate or offensive, and cannot be substantiated.

8.1. Electronic Hardware

- All hardware held within school should be included on the asset register;
- When an item is replaced, the register should be updated with the new equipment removed or replaced;
- Do not let anyone remove equipment unless you are sure that they are authorised to do so;

Homeworking Guidance

If staff must work outside of the school or at home, all of the 'Information Security' policy principles still apply. However, working outside of the school presents increased risks for securing information. The following additional requirements apply:

- Do not access confidential information when you are in a public place, such as a train and may be overlooked;
- Do not have conversations about personal or confidential information on your mobile when in a public place. Ensure that, if urgent, you have your conversation in a separate room or away from other people;
- The remote desktop should be used so confidential documents do not have to be taken off side whenever possible so data is still being held securely on the school servers.

If you use a laptop or tablet or smart phone:

- Ensure that it is locked and password protected to prevent unauthorised access;
- Make sure that you don't leave your device anywhere it could be stolen. Keep it with you at all times and secure it when you are in the School;
- Portable devices or memory sticks that contain personal data must be encrypted. Personal data may not be taking off the school's site or put onto a portable devise without the express permission of the Headteacher. Taking personal data off-site on a device or media that is not encrypted is a disciplinary matter;
- Ensure personal data is not stored on the hard drive;
- When working on confidential documents at home do not leave them lying around where others may see them; dispose of documents using a shredder;
- If you are using your own computer, ensure that you access and work on your school computer using the Remote Desktop. Do not transfer documents and data to your own machine. It is forbidden to use a computer owned by you to hold personal data about pupils or staff at the school.

Audit of Data Access

- Where possible our software specifications will include the function to audit access to confidential data and attribute access, including breaches of security, to specific users.

Data Backup

- The school will arrange that all critical and personal data is backed up to physical storage. If the school is physically damaged critical data backups in a remote location will allow the Trust to continue its business at another location with secure data.
- Data backup should routinely be managed on a rolling daily process to secure off-site areas.

9. Disposal of Information

- Paper records should be disposed of with care. If papers contain confidential or sensitive information they must be placed in the confidential bins for secure collection or shredded before disposing of them. Particular care must be taken when selecting papers to be placed in a recycling bin.
- Computers and hardware to be disposed of must be completely 'cleaned' before disposal. It is not enough just to delete all the files.
- It cannot be assumed that simply deleting a file will prevent it being recovered from electronic media. Electronic memory containing personal information or sensitive personal information

must be electronically scrubbed or physically destroyed.

- Where a third party contractor holds personal information on behalf of the school, for example a payroll provider, the school will seek reassurance from the contractor regarding their data protection policies and procedures.

10. Subject Access Requests

- Requests from parents or pupils for access to personal data or educational records will be dealt with as described in the Privacy Notice for Pupils and their Parents and Guardians.
- School staff may have access to their personal data within 40 calendar days of a request and at no charge.
- The school will maintain a documented record of all requests for personal information with details of who dealt with the request, what information was provided and when, and any outcomes. The record will be used if there is a subsequent complaint in relation to the request.

11. Sharing Personal Information

- The school only shares personal information with other organisations where there is a legal requirement to do so or the organisation has been contracted by the School Trust to carry out a function of the school.
- The school is required, for example, to share information with the Department for Education and the Education Funding Agency. Under certain circumstances, such as child protection, we may also be required to share information with Children's Social Services or the police.
- Because our pupils are of secondary school age, their own right to access their own personal information held by the school will be exercised through their parents or guardians.
- The Headteacher will be responsible for authorising the sharing of data with another organisation. The principle, in authorising the sharing of data will take account of:
- Whether it is lawful to share it;
- Whether there is adequate security in place to protect the information while it is being transferred and then held by the other organisation;
- Include in the Privacy Notice a simple explanation of who the information is being shared with and why.

Considerations regarding the method of transferring data should include:

- If personal data is sent by e-mail then security will be threatened. You may need to check that the recipient's arrangements are secure enough before sending the message. The data may also need to be password protected and the password sent separately. You should also check that it is going to the correct e-mail address.
- Circular e-mails sent to parents should be sent bcc (blind carbon copy) so that the e-mail addresses are not disclosed to everyone.
- Similar considerations apply to the use of fax machines. Ensure that the recipient will be present to collect a fax when it is sent and that it will not be left unattended on their equipment.
- If confidential personal data is provided by paper copy it is equally important to ensure that it reaches the intended recipient.

12. Websites

- The school website will be used to provide important information for parents and pupils including our Privacy Notice and our Freedom of Information publication scheme.
- Where personal information, including images, are placed on the web site the following principles will apply:
- We will not disclose personal information (including photos) on a web site without the consent of the pupil, parent, member of staff or Governor as appropriate;

- Comply with regulations regarding cookies and consent for their use;
- Our website design specifications will take account of the principles of data protection.

13. CCTV

If the school uses CCTV this will be notified to the Information Commissioners Office along with the purpose of capturing images using CCTV. The school appreciates that images captured on CCTV constitute personal information under the Data Protection Act.

14. Photographs

- The school may use photographs of pupils or staff taken for inclusion in the printed prospectus or other school publications without further specific consent being sought.
- Images recorded by parents using their own personal equipment of their child in a school play or activity for their own family use are not covered by data protection law.
- All other uses by the school of photographic images are subject to data protection.

15. Processing by Others

The school remains responsible for the protection of data that is processed by another organisation on its behalf. As part of a contract of engagement other organisations that process data on behalf of the school will have to specify how they will ensure compliance with data protection law.

16. Training

The Headteacher will ensure that all staff are adequately trained to understand their responsibilities in relation to this policy and procedures.

B

Data Retention

Storage and Disposal

Plan and Policy - Specific

This policy forms part of the Overarching Data Protection Policy and Procedure.

1. Legal and Regulatory Framework

The following legal and regulatory framework should be considered in connection this this policy:

- The Data Protection Act 1998
- The Privacy and Electronic Communications Regulations 2011
- The Protection of Freedoms Act 2012
- GDPR – March 2018

In addition the relevant guidance and practice notes provided by the Information Commissioner's Office is as follows:

- The ICO Guide to the Privacy and Electronic Communications Regulations
- The ICO Guide to Direct Marketing
- The ICO Code of Practice on Subject Access
- The ICO Code of Practice on CCTV
- The ICO Code of Practice on Privacy Notices
- The ICO sector-specific guidance for schools, universities and colleges.

1.1 St Bede's Catholic Academy is required to process relevant personal data regarding staff and pupils as part of its operation and shall take all reasonable steps to do so in accordance with this policy. In accordance with the Data Protection Act 1998 ("the Act"), the School has notified the Information Commissioner's Office of its processing activities. The School's ICO registration number is Z9863314 and its registered address is St Bede's Catholic School and Sixth Form College, Consett Road, Lanchester, Co. Durham. DH7 0RD.

1.2 The School has appointed the Director of Academy Services as the Data Protection Officer (DPO), who will endeavour to ensure that all personal data is processed in compliance with this policy and the Act.

1.3 The DPA applies to both paper-based/non-electronic and computer/automated collections of personal data.

1.4 St Bede's Catholic School and Sixth Form College shall, so far as is reasonably practicable, comply with the Data Protection Principles (the Principles) contained in the Data Protection Act to ensure all data is:

A. fairly and lawfully processed;
B. processed for a lawful purpose;
C. adequate, relevant and not excessive;
D. accurate and up to date;
E. not kept for longer than necessary;
F. processed in accordance with the data subject's rights;
G. secure;
H. not transferred to other countries without adequate protection.

2. **Personal Data Processed by the School**

2.1 The School may process a wide range of personal data about individuals including current, past and prospective pupils and their parents as part of its operation, including by way of example :

- names, addresses, telephone numbers, e-mail addresses and other contact details;
- car details (about those who use our car parting facilities);
- bank details and other financial information, e.g. about parents who pay fees to the school;
- past, present and prospective pupils' academic, disciplinary, admissions and attendance records (including information about any special needs), and examination scripts and marks;
- where appropriate, information about individuals' health, and contact details for their next of kin;
- references given or received by the school about pupils, and information provided by previous educational establishments and/or other professionals or organisations working with pupils;
- images of pupils (and occasionally other individuals) engaging in school activities, and images captured by the school's CCTV system (in accordance with the School's policy on taking, storing and using images of children);

2.2 Generally, the School receives personal data from the individual directly (or, in the case of pupils, from parents). However, in some cases personal data may be supplied by third parties (for example another school, other professionals or authorities working with that individual), or collected from publicly available resources.

2.3 The School may, from time to time, need to process sensitive personal data regarding individuals. Sensitive personal data and includes information about an individual's psychical or mental health, race of ethnic origin, political or religious beliefs, sex life, trade union membership or criminal records and proceedings. Sensitive personal data is entitled to special protection under the Act, and will only be processed by the School with the explicit consent of the appropriate individual, or as otherwise permitted by the Act.

3. **Purposes for which Personal Data may be processed**

3.1 The School will use (and, where appropriate share with third parties) personal data about individuals for a number of purposes as part of its operation, including as follows;

- for the purposes of pupil selection and to confirm the identity of prospective pupils and their parents;
- to provide education services (including SEN), career services, and extra-curricular activities to pupils; monitoring pupils' progress and educational needs;
- for the purpose of management planning and forecasting, research and statistical analysis, and to enable the relevant authorities to monitor the School's performance;
- to give and receive information and reference about past, current and prospective pupils, including relating to outstanding fees or payment history, to/from any educational

institution that the pupil attended or where it is proposed they attend; and to provide references to potential employers of past pupils.

- to enable pupils to take part in national or other assessments, and to publish the results of public examinations or other achievements of pupils of the School.
- to safeguard pupils' welfare and provide appropriate pastoral (and where necessary, medical) care, and to take appropriate action in the event of an emergency or accident, including by disclosing details of an individual's medical condition where it is in the individual's interests to do so, e.g. for medical advice, insurance purposes or to organisers of school trips.
- to monitor (as appropriate) use of the School's IT and communications systems in accordance with the School's IT, acceptable use policy.
- to make use of photographic images of pupils in School publications, on the school website and (where appropriate) on the School's social media channels in accordance with the school's policy on taking, storing and using images of children.
- for security purposes, and for regulatory and legal purposes (e.g. child protection and health and safety) and to comply with its legal obligations.
- Where otherwise reasonably necessary for the school's purposes, including to obtain appropriate professional advice and insurance for the school.

4. **Access by Staff**

4.1 All teaching and office staff are able to access the School's password protected database. Access to certain data within the database, including medical and financial, is restricted only to those who require it to fulfil their duties.

5. **Rights to access Personal Data** (mindful of GDPR March 2018)

5.1 Individuals have the right under the Act of access to personal data about them held by the School, subject to certain exemptions and limitations set out in the Act. Any individual wishing to access their personal data should put their request in writing to the DPO.

5.2 The School will endeavour to respond to any such written requests (known as subject access requests) as soon as is reasonably practicable and in any event within statutory time-limits of 40 days. The School may charge an administration fee for providing this information.

5.3 Certain data is exempt from the right of access under the Act. This may include information which identifies other individuals, or information which is subject to legal professional privilege. The School is also not required to disclose any pupil examination scripts (though examiners' comments may fall to be disclosed), nor any reference given by the School for the purposes of education, training or employment of any individual.

5.4 Pupils can make subject access requires for their own personal data, provided that, in the reasonable opinion of the School, they have sufficient maturity to understand the request they are making. Pupils aged over 12 or over are generally assumed to have this level of maturity, although this will depend on both the child and the personal data requested. All subject access requests from pupils will therefore be considered on a case by case basis.

5.5 A person with parental responsibility will generally be expected to make a subject access request on behalf of younger pupils. A pupil of any age may ask a parent or other representative to make a subject access request on his/her behalf.

6 Data Accuracy and Security

6.1 The School will endeavour to ensure that all personal data held in relation to an individual is as up to date and accurate as possible. Individuals must notify the School of any changes to information held about them.

6.2 An individual has the right to request that inaccurate information about them is erased or corrected (subject to certain exemptions and limitations under the Act) and may do so by contacting the DPO in writing.

6.3 The School will take appropriate technical and organisational steps to ensure the security of personal data about individuals. All staff will be made aware of this policy and their duties under the Act.

7 Staff Training

7.1 High-profile security breaches have increased public concern about the handling of personal information. As some 80% of security incidents involve staff, there is a clear need for all staff to have a basic understanding the Data Protection Act 1998 (DPA). Data Protection is a regular topic of discussion at staff meetings and briefings.

8 Data Retention

8.1 St Bede's Catholic School & Sixth form College generally seeks to balance the benefits of keeping detailed and complete records – for the purposes of good practice, archives or general reference – with practical considerations of what is reasonable and of storage, space and accessibility. We are mindful of the legal consideration in respect of retention of records and documents which include:

- statutory duties and government guidance relating to schools;
- the law of confidentiality and privacy;
- disclosure requirements in the course of litigation;
- contractual obligations;
- the Data Protection Act (DPA).

These will inform not only minimum and maximum retention periods, but also what to keep and how to keep it.

8.2 Meaning of Record

For the purposes of this policy a record means any document or item of data which contains evidence or information relating to the School, its staff or pupils. Some of this material will contact personal data of individuals as defined in the DPA, but not all.

Many, if not most, new and recent records will be created, received and stored electronically. Others (such as certificates, registers or older records) will be original paper documents. The format of the records is less important that its contents and the purpose for keeping it.

<u>Digital records</u>

Digital records can be lost or misappropriated in huge quantities very quickly. Access to sensitive data, or any large quantity of data, will be wherever possible password-protected and held on a limited number of devices only, with passwords provided on a need-to-know basis and regularly changed.

E-mails (whether they are retained electronically or printed out as part of a paper file) are also records and may be particularly important; whether as disclosable documents in any litigation or as representing personal data of the sender (or subject) for data protection/data privacy purposes. Again, however, the format is secondary to the content and the purpose of keeping the document as a record.

Paper records

Paper records will wherever possible be stored in dry secure conditions. Staff procedures are in place to archive paper records to a central facility within school at certain times of the year.

8.3 **Archiving and the destruction or erasure of records**

All staff receive basic training in data management and on issues such as security, recognising and handling sensitive personal data, safeguarding, etc. Staff given specific responsibility for the management of records must have specific training and ensure, as a minimum, the following:

- that records, - whether electronic or hard copy – are stored securely as above, so that access is available only to authorised personal and the records themselves are available when required and (where necessary) searchable.
- that important records, and large or sensitive personal databases, are not taken home or – in respect of digital data – carried or kept on portable devices (whether CDs or data sticks, or mobiles and handheld electronic tablets) unless absolutely necessary.
- that questions of back-up or migration are likewise approached in line with general school policy (such as professional storage solutions or IT systems) and not individual ad hoc action.
- that arrangements with external storage providers – whether physical or electronic (in any form, but most particularly could-based storage) – are supported by robust contractual arrangements providing for security and access.
- that reviews are conducted on a regular basis, in line with the guidance below, to ensure that all information being kept is still relevant and – in the case of personal data – necessary for the purposes for which it is held (and if so, that it is accurate and up-to-date).
- that all destruction or permanent erasure of records, if undertaken by a third party, is carried out securely – with no risk of the re-use or disclosure, or re-construction, of any records or information contained in them.

8.4 **Retention Periods**

Type of Record/Document	Retention Period
School Specific Records	
- Registration documents of the school	Permanent (or until closure of the school)
- Attendance Register	6 years from last date of entry, then archive
- Minutes of Governors' meetings	6 years from date of meeting
- Annual curriculum	From end of year: 3 years (or 1 year for other class records ; eg. Marks/timetables/assignments

<u>Individual Pupil Records</u> - Admissions: application forms, assessments, records of decisions - Examination results (external or internal) Pupil file including : Pupil reports Pupil performance records Pupil medical records Special Educational Needs records (*to be risk assessed individually)*	25 years from date of birth (or, if pupil not admitted, up to 7 years from that decision). 7 years from pupil leaving school. All : 25 years from date of birth* **unless there is good reason to consider this may be applicable evidence in a medical negligence or abuse claim:* see "safeguarding" below Date of birth plus up to 35 years (allowing for special extensions to statutory limitation period)
<u>Safeguarding</u> - Policies and procedures - Incident reporting	Keep a permanent record of historic policies Keep on record for 35 years ideally reviewed regularly (eg. Every 6 years) if a suitably qualified person is available <u>and</u> resources allow. **
Limitation periods can be disapplied in criminal or civil abuse cases. However, rights under the DPA and insurers' requirements remain relevant	** Courts may be sympathetic if not, but the ICO (Information Commissioner's Office) will expect to see a responsible assessment policy in place.
<u>Corporate Records (Where applicable)</u> - Certificates of Incorporation - Minutes, Notes and resolutions of Boards or Management Meetings - Shareholder resolutions - Register of Members/Shareholders - Annual reports	Permanent (or until dissolution of the company) Minimum – 10 years Minimum – 10 years Permanent (minimum 10 years for ex-members / shareholders) Minimum – 6 years
<u>Accounting Records</u> - Accounting records (*normally taken to mean records which enable a company's accurate financial position to be ascertained and which give a true and fair view of the company's financial state)* NB <u>specific ambit to be advised by an accountancy expert.</u> - Tax returns - VAT returns - Budget and internal financial reports	Minimum – 3 years for private UK companies (except where still necessary for tax returns) Minimum – 6 years for UK charities (and public companies) from the end of the financial year in which the transaction took place. Minimum – 6 years Minimum – 6 years Minimum – 3 years

<u>Contracts and agreements</u> - Signed or final/concluded agreements (*plus any signed or final/concluded variations or amendments)* - Deeds (or contracts under seal)	Minimum – 7 years from completion of contractual obligations or term of agreement, whichever is the later. Minimum – 13 years from completion of contractual obligation or term of agreement
<u>Intellectual Property Records</u> - Formal documents of title (trade mark or registered design certificates; patent or utility model certificates) - Assignments of intellectual property to or from the school - IP/IT agreements (including software licences and ancillary agreements e.g. maintenance; storage; development; co-existence agreements; consents)	Permanent (in the case of any right which can be permanently extended, e.g. trade marks); otherwise expiry of right plus minimum of 7 years As above in relation to contracts (7 years) or, where applicable, deeds (13 years) Minimum – 7 years from completion of contractual obligation concerned or term of agreement.
<u>Employee/Personnel Records</u> - Contracts of employment - Employee appraisals or reviews and staff personnel file - Payroll, salary, maternity pay records - Pension or other benefit schedule records - Job application and interview/rejection records (unsuccessful applicants) - Immigration records - Health records relating to employees	**NB This will almost certainly be personal data** Minimum – 7 years from effective date of end of contact. Duration of employment plus minimum 7 years Minimum – 6 years Possible permanent, depending on nature of scheme. Minimum – 3 years Minimum – 4 years Minimum of 7 years from end of contract of employment.
<u>Insurance Records</u> Insurance policies (will vary – private, public, professional indemnity) Correspondence related to claims/ renewals/ notification re: insurance.	Duration of policy (or as required by policy) plus a period for any run-off arrangement and coverage of insured risks: ideally, until it is possible to calculate that no living person could make a claim Minimum – 7 years
<u>Environmental and Health Records</u> - Maintenance logs - Accidents to children	10 years from date of last entry 25 years from birth (unless safeguarding incident)

- Accident at work records (staff) - Staff use of hazardous substances - Risk assessments (carried out in respect of above)	Minimum – 4 years from date of accident, but review case by case where possible. Minimum – 7 years from end of date of use 7 years from completion of relevant project, indecent, event or activity.

NB. The Goddard Inquiry needs to be taken into consideration when considering data retention and disposal.

9 **Cloud Storage and Data Protection**

9.1 As part of its ICT Infrastructure St Bede's Catholic School and Sixth Form College uses Microsoft Office 365 which utilises a cloud based storage system. Likewise, the School backs up the data on its network using a cloud-based service provided by Microsoft, called Windows Azure (the School has a written agreement with Microsoft providing security compliance and assurances that data sorted are secure). Microsoft guarantees school data are stored within the EEC (Ireland or the Netherlands).

C

Security Breach Management

Plan and Policy - Specific

St Bede's Catholic Academy (Lanchester) is committed to maintaining the confidentiality of its information and ensuring that the details of the finances, operation and individuals within the schools are only accessible by the appropriate individuals. It is therefore important to uphold high standards of security and precaution, and to have systems and procedures in place that support this – such as the E-security Policy.

The Academy recognises, however, that breaches in security can occur, particularly as the majority of information is stored online or on electronic devices which are increasingly vulnerable to cyber-attacks. This being the case, it is necessary to have a contingency plan, and procedures in place to minimise the potential negative impacts of any security breach, to alert the relevant authorities, and to take steps to help prevent a repeat occurrence.

For the purposes of the policy, the title of "**data controller**" will be used in reference to the person(s) primarily responsible for handling of information and data within a school.

Legal Framework

This policy has due regard to statutory legislation and regulations, including but not limited to :

- The Data Protection Act 1998;
- The computer Misuse Act 1990;
- The General Data Protection Regulation (GDPR), came into effect from 25th May 2018.

This policy also has due regard to Trust and school policies and procedures, including but not limited to:

- E-Security Policy;
- E-Safety Policy;
- Data Protection Policy.

Enacting the Security Breach Management Plan

Data security breaches require more than just an immediate response to identify and contain the situation; they also require longer-term recovery planning. This will pull together the views and expertise of various individuals and groups from across the school or Trust – input may be necessary from IT, HR and legal services, and in some cases from external authorities, stakeholders and suppliers.

These processes are start once the breach has been detected, with the initial procedure being run in the following four-step process – containment and recovery, assessment of risks, consideration of further notification, and evaluation and response.

Containment and Recovery

The data controller/IT lead and Headteacher for the school, will take the lead in investigating the breach, and will be allocated the appropriate time and resources to conduct this.

As soon as reasonably possible, the data controller will ascertain the severity of the breach and determine if any personal data is involved or compromised. They will oversee a full investigation and produce a comprehensive report.

The cause of the breach, and whether or not it has been contained, will be identified, ensuring that the possibility of further loss/jeopardising of data is eliminated or restricted as much as possible.

Any further action which could be taken to recover lost or damaged data will be identified. This includes the physical recovery of data, as well as the use of back-ups.

The school will establish what steps need to be taken to prevent further data loss which will require support from various school departments and staff. This action will include:

- Informing relevant staff of their roles and responsibilities in areas of the containment process;
- Taking systems offline;
- Retrieving any lost, stolen or otherwise unaccounted for data;
- Retrieving access to systems entirely or to a small group;
- Backing up all existing data and storing it in a safe location;
- Reviewing basic security, including
    - Changing passwords and login details on electronic equipment;
    - Ensuring access to places where electronic or hard data is kept is monitored and requires authorisation.

Where appropriate, e.g. if offences have been committed under the Computer Misuse Act 1990, the data controller will inform the policy of the security breach.

Assessment of Risks

The following questions will be considered by the data controller in order to fully and effectively assess the risks that the security breach has brought, and to help take the next appropriate steps. All relevant questions should be clearly and fully answered in the data controller's report and records.

- What type and how much data is involved?
- How sensitive is the data? Sensitive data is defined in the Data Protection Act 1998; some data is sensitive because of its very personal nature (e.g. health records) while other data types are sensitive because of what might happen if it is misused (e.g. bank account details).
- It is possible to identify what has happened to the data – has it been lost/stolen/deleted/ tampered with?
- If the data has been lost/stolen, were there any protective measures in place to prevent this, such as data and device encryption?
- If the data has been compromised, have there been effective measures in place to mitigate the impact of this, such as the creation of back-up tapes and spare copies?
- Has the individuals' personal data been compromised – how many individuals are affected?
- Who are these individuals – are they pupils, staff, governors, volunteers, stakeholders, suppliers?
- Could their information be misused or manipulated in any way?

- Could harm come to individuals? This could include risks to the following:
    - Physical safety;
    - Emotional wellbeing;
    - Reputation;
    - Finances;
    - Identify;
    - Private affairs.
- Are there further implications beyond the risks to individuals? Is there a risk of loss of public confidence/damage to the school's reputation, or risk to the school's operations?
- Who could help or advise the school on the breach? Could the LA, external partners, authorities, or others provide effective support?

In the event that the data controller or other persons involved in assessing the risks to the school are not confident in the risk assessment, they will seek advice from the Information Commissioner's Office (ICO).

Consideration of Further Notification

The school will consider whether there are any legal, contractual or regulatory requirements to notify individuals or organisations that may be affected or who will have an interest in security. This includes any specific GDPR requirements about personal data, as set out at the of this section.

The school will decide whether notification will help the school meet its statutory obligations under the seventh data protection principle.

The school will assess whether notification could help the individual(s) affected, and whether individuals could act on the information provided to mitigate risks, e.g. by cancelling a credit card or changing a password.

It a large number of people are affected, or there are very serious consequences, the ICO will be informed.

The school will consider whom to notify, what to tell them and how they will communicate the message, which may include:

- A description of how and when the beach occurred and what data was involved. Details of what has already been done to respond to the risks posed by the breach will be included;
- Specific and clear advice on the steps they can take to protect themselves, and what the school is willing to do to help them;
- How they can contact the school for further information or to ask questions about what has occurred.

The school will conduct the ICO for guidance on when and how to notify them about breaches.

The school will consider, as necessary, the need to notify any third parties (e.g. police, insurers, professional bodies, funders, trade unions, website/system owners, bank/credit card companies) who can assist in helping or mitigating the impact on individuals.

Steps to be taken under the GDPR for Breaches of Personal Data.

The school will notify the ICO within 72 hours of a breach where it is likely to result in a risk to the rights and freedoms of individuals. Where a breach is likely to result in a high risk to the rights and freedoms of individuals, the school will notify those concerned directly with the breach.

Where the breach compromises personal information, the notification will contain:

- The nature of the personal data breach including, where possible
    - The type(s) (e.g. pupils or governors) and approximate number of individuals concerned.
    - The type(s) and approximate number of personal data records concerned
- The name and contact details of the data controller or other person(s) responsible for handling the school's information;
- A description of the likely consequences of the personal data breach;
- A description of the measures taken, or proposed, to deal with and contain the breach and, where appropriate, the measures taken to mitigate any possible adverse effects.

Evaluation and Response

The data controller will;

- Establish the root of the breach, and where any present or future risks lie;
- Consider the data and contexts involved;
- Work with the Headteacher to identify any weak points in existing security measures and procedures and any weak points in levels of security awareness and training;
- Report on findings and, with approval of school leadership, implement the recommendations of the report after analysis and discussion.

Monitoring and Review

This policy will be reviewed the Headteacher, in conjunction with the data controller, on an annual basis.

The data controller is responsible for monitoring the effectiveness of this policy, amending necessary procedures and communication any changes to staff members.

Appendix A – Timeline of Incident Management

Date	Time	Activity	Decision	Name/Position	Date
