General Data Protection Policy
St Benedict's Catholic High School

Approved by:	Mr John McQuirk Chair of Governors	**Date:** 10th December 2020
Last reviewed on:	December 2020	
Next review due by:	December 2022	

Contents

1. Aims

Our school aims to ensure that all personal data collected about staff, pupils, parents, governors, visitors and other individuals is collected, stored and processed in accordance with the General Data Protection Regulation (GDPR) and the expected provisions of the Data Protection Act 2018 (DPA 2018) as set out in the Data Protection Bill.

This policy applies to all personal data, regardless of whether it is in paper or electronic format.

2. Legislation and guidance

This policy meets the requirements of the GDPR and the expected provisions of the DPA 2018. It is based on guidance published by the Information Commissioner's Office (ICO) on the GDPR and the ICO's code of practice for subject access requests.

It meets the requirements of the Protection of Freedoms Act 2012 when referring to our use of biometric data.

It also reflects the ICO's code of practice for the use of surveillance cameras and personal information.

In addition, this policy complies with regulation 5 of the Education (Pupil Information) (England) Regulations 2005, which gives parents the right of access to their child's educational record.

3. Definitions

Term	Definition
Personal data	Any information relating to an identified, or identifiable, individual. This may include the individual's: • Name (including initials) • Identification number • Location data • Online identifier, such as a username It may also include factors specific to the individual's physical, physiological, genetic, mental, economic, cultural or social identity.
Special categories of personal data	Personal data which is more sensitive and so needs more protection, including information about an individual's: • Racial or ethnic origin • Political opinions • Religious or philosophical beliefs • Trade union membership • Genetics • Biometrics (such as fingerprints, retina and iris patterns), where used for identification purposes • Health – physical or mental • Sex life or sexual orientation

Processing	Anything done to personal data, such as collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing or destroying. Processing can be automated or manual.
Data subject	The identified or identifiable individual whose personal data is held or processed.
Data controller	A person or organisation that determines the purposes and the means of processing of personal data.
Data processor	A person or other body, other than an employee of the data controller, who processes personal data on behalf of the data controller.
Personal data breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.

4. The data controller

Our school processes personal data relating to parents, pupils, staff, governors, visitors and others, and therefore is a data controller.

The school is registered as a data controller with the ICO and will renew this registration annually or as otherwise legally required.

5. Roles and responsibilities

This policy applies to **all staff** employed by our school, and to external organisations or individuals working on our behalf. Staff who do not comply with this policy may face disciplinary action.

5.1 Governing board

The governing board has overall responsibility for ensuring that our school complies with all relevant data protection obligations.

5.2 Data protection officer

The data protection officer (DPO) is responsible for overseeing the implementation of this policy, monitoring our compliance with data protection law, and developing related policies and guidelines where applicable.

They will provide an annual report of their activities directly to the governing board and, where relevant, report to the board their advice and recommendations on school data protection issues.

The DPO is also the first point of contact for individuals whose data the school processes, and for the ICO.

Full details of the DPO's responsibilities are set out in their job description.

Our DPO is Steve Bridgman and is contactable via steve.bridgman@st-benedicts.cumbria.sch.uk

5.3 Headteacher

The headteacher acts as the representative of the data controller on a day-to-day basis.

5.4 All staff

Staff are responsible for:

- Collecting, storing and processing any personal data in accordance with this policy
- Informing the school of any changes to their personal data, such as a change of address

- Contacting the DPO in the following circumstances:
    - With any questions about the operation of this policy, data protection law, retaining personal data or keeping personal data secure
    - If they have any concerns that this policy is not being followed
    - If they are unsure whether or not they have a lawful basis to use personal data in a particular way
    - If they need to rely on or capture consent, draft a privacy notice, deal with data protection rights invoked by an individual, or transfer personal data outside the European Economic Area
    - If there has been a data breach
    - Whenever they are engaging in a new activity that may affect the privacy rights of individuals
    - If they need help with any contracts or sharing personal data with third parties

6. Data protection principles

The GDPR is based on data protection principles that our school must comply with.

The principles say that personal data must be:

- Processed lawfully, fairly and in a transparent manner
- Collected for specified, explicit and legitimate purposes
- Adequate, relevant and limited to what is necessary to fulfil the purposes for which it is processed
- Accurate and, where necessary, kept up to date
- Kept for no longer than is necessary for the purposes for which it is processed
- Processed in a way that ensures it is appropriately secure

This policy sets out how the school aims to comply with these principles.

7. Collecting personal data

7.1 Lawfulness, fairness and transparency

We will only process personal data where we have one of 6 'lawful bases' (legal reasons) to do so under data protection law:

- The data needs to be processed so that the school can **fulfil a contract** with the individual, or the individual has asked the school to take specific steps before entering into a contract
- The data needs to be processed so that the school can **comply with a legal obligation**
- The data needs to be processed to ensure the **vital interests** of the individual e.g. to protect someone's life
- The data needs to be processed so that the school, as a public authority, can perform a task **in the public interest,** and carry out its official functions
- The data needs to be processed for the **legitimate interests** of the school or a third party (provided the individual's rights and freedoms are not overridden)
- The individual (or their parent/carer when appropriate in the case of a pupil) has freely given clear **consent**

For special categories of personal data, we will also meet one of the special category conditions for processing which are set out in the GDPR and Data Protection Act 2018.

If we offer online services to pupils, such as classroom apps, and we intend to rely on consent as a basis for processing, we will get parental consent where the pupil is under 13 (except for online counselling and preventive services).

Whenever we first collect personal data directly from individuals, we will provide them with the relevant information required by data protection law.

7.2 Limitation, minimisation and accuracy

We will only collect personal data for specified, explicit and legitimate reasons. We will explain these reasons to the individuals when we first collect their data.

If we want to use personal data for reasons other than those given when we first obtained it, we will inform the individuals concerned before we do so, and seek consent where necessary.

Staff must only process personal data where it is necessary in order to do their jobs.

When staff no longer need the personal data they hold, they must ensure it is deleted or anonymised. This will be done in accordance with the school's record retention policy.

8. Sharing personal data

We will not normally share personal data with anyone else, but may do so where:

- There is an issue with a pupil or parent/carer that puts the safety of our staff at risk
- We need to liaise with other agencies – we will seek consent as necessary before doing this
- Our suppliers or contractors need data to enable us to provide services to our staff and pupils – for example, IT companies. When doing this, we will:
    - Only appoint suppliers or contractors which can provide sufficient guarantees that they comply with data protection law
    - Establish a data sharing agreement with the supplier or contractor, either in the contract or as a standalone agreement, to ensure the fair and lawful processing of any personal data we share
    - Only share data that the supplier or contractor needs to carry out their service, and information necessary to keep them safe while working with us

We will also share personal data with law enforcement and government bodies where we are legally required to do so, including for:

- The prevention or detection of crime and/or fraud
- The apprehension or prosecution of offenders
- The assessment or collection of tax owed to HMRC
- In connection with legal proceedings
- Where the disclosure is required to satisfy our safeguarding obligations
- Research and statistical purposes, as long as personal data is sufficiently anonymised or consent has been provided

We may also share personal data with emergency services and local authorities to help them to respond to an emergency situation that affects any of our pupils or staff.

Where we transfer personal data to a country or territory outside the European Economic Area, we will do so in accordance with data protection law.

9. Subject access requests and other rights of individuals

9.1 Subject access requests

Individuals have a right to make a 'subject access request' to gain access to personal information that the school holds about them. This includes:

- Confirmation that their personal data is being processed
- Access to a copy of the data
- The purposes of the data processing
- The categories of personal data concerned
- Who the data has been, or will be, shared with
- How long the data will be stored for, or if this isn't possible, the criteria used to determine this period
- The source of the data, if not the individual
- Whether any automated decision-making is being applied to their data, and what the significance and consequences of this might be for the individual

Subject access requests should include:

- Name of individual

- Correspondence address
- Contact number and email address
- Details of the information requested

If staff receive a subject access request they must immediately forward it to the DPO.

9.2 Children and subject access requests

Personal data about a child belongs to that child, and not the child's parents or carers. For a parent or carer to make a subject access request with respect to their child, the child must either be unable to understand their rights and the implications of a subject access request, or have given their consent.

Children aged 12 and above are generally regarded to be mature enough to understand their rights and the implications of a subject access request. Therefore, most subject access requests from parents or carers of pupils at our school may not be granted without the express permission of the pupil. This is not a rule and a pupil's ability to understand their rights will always be judged on a case-by-case basis.

9.3 Responding to subject access requests

When responding to requests, we:

- May ask the individual to provide 2 forms of identification
- May contact the individual via phone to confirm the request was made
- Will respond without delay and within 1 month of receipt of the request
- Will provide the information free of charge
- May tell the individual we will comply within 3 months of receipt of the request, where a request is complex or numerous. We will inform the individual of this within 1 month, and explain why the extension is necessary

We will not disclose information if it:

- Might cause serious harm to the physical or mental health of the pupil or another individual
- Would reveal that the child is at risk of abuse, where the disclosure of that information would not be in the child's best interests
- Is contained in adoption or parental order records
- Is given to a court in proceedings concerning the child

If the request is unfounded or excessive, we may refuse to act on it, or charge a reasonable fee which takes into account administrative costs.

A request will be deemed to be unfounded or excessive if it is repetitive, or asks for further copies of the same information.

When we refuse a request, we will tell the individual why, and tell them they have the right to complain to the ICO.

9.4 Other data protection rights of the individual

In addition to the right to make a subject access request (see above), and to receive information when we are collecting their data about how we use and process it (see section 7), individuals also have the right to:

- Withdraw their consent to processing at any time
- Ask us to rectify, erase or restrict processing of their personal data, or object to the processing of it (in certain circumstances)
- Prevent use of their personal data for direct marketing
- Challenge processing which has been justified on the basis of public interest
- Request a copy of agreements under which their personal data is transferred outside of the European Economic Area
- Object to decisions based solely on automated decision making or profiling (decisions taken with no human involvement, that might negatively affect them)
- Prevent processing that is likely to cause damage or distress
- Be notified of a data breach in certain circumstances

- Make a complaint to the ICO
- Ask for their personal data to be transferred to a third party in a structured, commonly used and machine-readable format (in certain circumstances)

Individuals should submit any request to exercise these rights to the DPO. If staff receive such a request, they must immediately forward it to the DPO.

10. Parental requests to see the educational record

Parents, or those with parental responsibility, have a legal right to free access to their child's educational record (which includes most information about a pupil) within 15 school days of receipt of a written request.

11. Biometric recognition systems

Where we use pupils' biometric data as part of an automated biometric recognition system (for example, pupils use finger prints to receive school dinners instead of paying with cash), we will comply with the requirements of the Protection of Freedoms Act 2012.

Parents/carers will be notified before any biometric recognition system is put in place or before their child first takes part in it. The school will get written consent from at least one parent or carer before we take any biometric data from their child and first process it.

Parents/carers and pupils have the right to choose not to use the school's biometric system(s). We will provide alternative means of accessing the relevant services for those pupils by issuing an individual pin number. For example, pupils can pay for school dinners in cash using the reval machines and using their individual pin number at each transaction if they wish.

Parents/carers and pupils can object to participation in the school's biometric recognition system(s), or withdraw consent, at any time, and we will make sure that any relevant data already captured is deleted.

As required by law, if a pupil refuses to participate in, or continue to participate in, the processing of their biometric data, we will not process that data irrespective of any consent given by the pupil's parent(s)/carer(s).

Where staff members or other adults use the school's biometric system(s), we will also obtain their consent before they first take part in it, and provide alternative means of accessing the relevant service if they object. Staff and other adults can also withdraw consent at any time, and the school will delete any relevant data already captured.

12. CCTV

We use CCTV in various locations around the school site to ensure it remains safe. We will adhere to the ICO's code of practice for the use of CCTV.

We do not need to ask individuals' permission to use CCTV, but we make it clear where individuals are being recorded. Security cameras are clearly visible and accompanied by prominent signs explaining that CCTV is in use.

Any enquiries about the CCTV system should be directed to Mr Steve Bridgman, Deputy Headteacher

13. Photographs and videos

As part of our school activities, we may take photographs and record images of individuals within our school.

We will obtain written consent from parents/carers, or pupils aged 18 and over, for photographs and videos to be taken of pupils for communication, marketing and promotional materials.

Where we need parental consent, we will clearly explain how the photograph and/or video will be used to both the parent/carer and pupil. Where we don't need parental consent, we will clearly explain to the pupil how the photograph and/or video will be used.

Uses may include:

- Within school on notice boards and in school magazines, brochures, newsletters, etc.
- Outside of school by external agencies such as the school photographer, newspapers, campaigns
- Online on our school website or social media pages

Consent can be refused or withdrawn at any time. If consent is withdrawn, we will delete the photograph or video and not distribute it further.

When using photographs and videos in this way we will not accompany them with any other personal information about the child, to ensure they cannot be identified.

See our E-Safety / IT acceptable use policy for more information on our use of photographs and videos.

14. Data protection by design and default

We will put measures in place to show that we have integrated data protection into all of our data processing activities, including:

- Appointing a suitably qualified DPO, and ensuring they have the necessary resources to fulfil their duties and maintain their expert knowledge
- Only processing personal data that is necessary for each specific purpose of processing, and always in line with the data protection principles set out in relevant data protection law (see section 6)
- Completing privacy impact assessments where the school's processing of personal data presents a high risk to rights and freedoms of individuals, and when introducing new technologies (the DPO will advise on this process)
- Integrating data protection into internal documents including this policy, any related policies and privacy notices
- Regularly training members of staff on data protection law, this policy, any related policies and any other data protection matters; we will also keep a record of attendance
- Regularly conducting reviews and audits to test our privacy measures and make sure we are compliant
- Maintaining records of our processing activities, including:
    - For the benefit of data subjects, making available the name and contact details of our school and DPO and all information we are required to share about how we use and process their personal data (via our privacy notices)
    - For all personal data that we hold, maintaining an internal record of the type of data, data subject, how and why we are using the data, any third-party recipients, how and why we are storing the data, retention periods and how we are keeping the data secure

15. Data security and storage of records

We will protect personal data and keep it safe from unauthorised or unlawful access, alteration, processing or disclosure, and against accidental or unlawful loss, destruction or damage.

In particular:

- Paper-based records and portable electronic devices, such as laptops and hard drives that contain personal data are kept under lock and key when not in use
- Papers containing confidential personal data must not be left on office and classroom desks, on staffroom tables, pinned to notice/display boards, or left anywhere else where there is general access
- Where personal information needs to be taken off site, staff must sign it in and out from the school office
- Passwords that are at least 8 characters long containing letters and numbers are used to access school computers, laptops and other electronic devices. Staff and pupils are reminded to change their passwords at regular intervals
- Encryption software is used to protect all portable devices and removable media, such as laptops and USB devices
- Staff, pupils or governors who store personal information on their personal devices are expected to follow the same security procedures as for school-owned equipment (see our E-Safety Policy / IT acceptable use guidance for school based staff.
- Where we need to share personal data with a third party, we carry out due diligence and take reasonable steps to ensure it is stored securely and adequately protected (see section 8)

16. Disposal of records

Personal data that is no longer needed will be disposed of securely. Personal data that has become inaccurate or out of date will also be disposed of securely, where we cannot or do not need to rectify or update it.

For example, we will shred or incinerate paper-based records, and overwrite or delete electronic files. We may also use a third party to safely dispose of records on the school's behalf. If we do so, we will require the third party to provide sufficient guarantees that it complies with data protection law.

17. Personal data breaches

The school will make all reasonable endeavours to ensure that there are no personal data breaches.

In the unlikely event of a suspected data breach, we will follow the procedure set out in appendix 1.

When appropriate, we will report the data breach to the ICO within 72 hours. Such breaches in a school context may include, but are not limited to:

- A non-anonymised dataset being published on the school website which shows the exam results of pupils eligible for the pupil premium
- Safeguarding information being made available to an unauthorised person
- The theft of a school laptop containing non-encrypted personal data about pupils

18. Training

All staff and governors are provided with data protection training as part of their induction process.

Data protection will also form part of continuing professional development, where changes to legislation, guidance or the school's processes make it necessary.

19. Monitoring arrangements

The DPO is responsible for monitoring and reviewing this policy.

This policy will be reviewed and updated if necessary when the Data Protection Bill receives royal assent and becomes law (as the Data Protection Act 2018) – if any changes are made to the bill that affect our school's practice. Otherwise, or from then on, this policy will be reviewed **every 2 years** and shared with the full governing board.

Note: the 2-year review frequency here reflects the information in the Department for Education's advice on statutory policies..

20. Links with other policies

This data protection policy is linked to our:

- Freedom of information act policy
- E-Safety/ IT acceptable use policy
- CCTV policy
- Safeguarding young people policy
- Attendance
- SEND policy
- Recruitment and Selection
- Behaviour and Standards
- Bullying/Cyber bullying

Privacy Notice

How we use student information

The categories of student information that we collect, hold and share include:

- Personal information (such as name, contact details, unique student numbers, student photograph);
- Characteristics (such as ethnicity, religion, language, nationality, country of birth, free school meal eligibility, and student premium eligibility);
- Safeguarding information (such as court orders and professional involvement)
- Special educational needs (including the needs and ranking)
- Medical and administration (such as doctors information, child health, any first aid or accident information, dental health, allergies, medication, dietary requirements and notes from meetings/GPs/other health care professionals)
- Attendance information (such as sessions attended, number of absences and absence reasons and any previous schools attended).
- Assessment and attainment information (such as Key Stage results, reports, feedback, test data, exam entries and results, post-16 courses enrolled for and any relevant results)
- Special Educational Needs information (such as Education and Health Care Plans (EHCPs), Student Support Plans, and notes from review meetings and professional assessments)
- Rewards information
- Behavioural information such as exclusions and any relevant alternative provision put in place
- Information on trips and visits, catering, free school meals management, identity management and authentication
- Mode of transport information
- Post 16 learning information and destination data

Why we collect and use this information

We use the student data for the following purposes:

- To support student learning;
- To monitor and report on student attainment progress;
- To provide appropriate pastoral care;
- To assess the quality of our services;
- To comply with the law regarding data sharing;
- To keep children safe (food allergies or emergency contact details)
- To meet statutory duties placed upon us for DfE data collections

The lawful basis on which we use this information

We collect and use student information for general purposes of the school GDPR policy which complies with Articles 6 and 9 of the GDPR.

In addition concerning any special category data:

- Conditions which comply with Article 9 of the GDPR.

How we collect student information

We collect student information via Sims Parent App when joining the school and refresh information throughout the time at the school and Common Transfer File (CTF) or secure file transfer from previous schools, local authorities and/or Department for Education (DfE).

Student data is essential for the school's operational use. Whilst the majority of student information you provide to us is mandatory, some of it is requested on a voluntary basis. In order to comply with the data

protection legislation, we will inform you at the point of collection, whether you are required to provide certain student information to us or if you have a choice in this.

How we store student data

We hold student data securely for the set amount of time shown in our data retention schedule. For more information on our data retention schedule and how we keep your data safe, please see our data retention schedule.

Who we share student information with

We routinely share student information with:

- other educational establishments that the students attend after leaving us;
- Cumbria County Council;
- The Department for Education (DfE);
- Other public services that have a lawful right to collect student information;
- Youth support services (students aged 13+);
- Third parties as listed in Appendix 6 of the GDPR policy;
- Inspira (for destinations data).
- The Public Health Department (for the organisation and administration of the agreed immunisation programmes)

We do not share information about our students with anyone without consent unless the law and our policies allow us to do so.

Why we share student information

We are required to share information about our students with our local authority (LA) and the Department for Education (DfE) under section 3 of The Education (Information About Individual Students) (England) Regulations 2013.

Data collection requirements:

To find out more about the data collection requirements placed on us by the Department for Education (for example; via the school census) go to https://www.gov.uk/education/data-collection-and-censuses-for-schools.

Collecting student information

Whilst the majority of student information you provide to us is mandatory, some of it is provided to us on a voluntary basis. In order to comply with the General Data Protection Regulation, we will inform you whether you are required to provide certain student information to us or if you have a choice in this.

Youth support services

Students aged 13+

Once our students reach the age of 13, we also pass student information to our local authority and / or provider of youth support services as they have responsibilities in relation to the education or training of 13-19 year olds under section 507B of the Education Act 1996.

This enables them to provide services as follows:

- youth support services
- careers advisers

A parent or guardian can request that **only** their child's name, address and date of birth is passed to their local authority or provider of youth support services by informing us. This right is transferred to the child / student once he/she reaches the age 16.

Students aged 16+

We will also share certain information about students aged 16+ with our local authority and / or provider of youth support services as they have responsibilities in relation to the education or training of 13-19 year olds under section 507B of the Education Act 1996.

This enables them to provide services as follows:

- post-16 education and training providers
- youth support services
- careers advisers

For more information about services for young people, please visit our local authority website.

The National Student Database (NPD)

The NPD is owned and managed by the Department for Education and contains information about students in schools in England. It provides invaluable evidence on educational performance to inform independent research, as well as studies commissioned by the Department. It is held in electronic format for statistical purposes. This information is securely collected from a range of sources including schools, local authorities and awarding bodies.

We are required by law, to provide information about our students to the DfE as part of statutory data collections such as the school census and early years' census. Some of this information is then stored in the NPD. The law that allows this is the Education (Information About Individual Students) (England) Regulations 2013.

To find out more about the NPD, go to https://www.gov.uk/government/publications/national-student-database-user-guide-and-supporting-information.

The department may share information about our students from the NPD with third parties who promote the education or well-being of children in England by:

- conducting research or analysis
- producing statistics
- providing information, advice or guidance

The Department has robust processes in place to ensure the confidentiality of our data is maintained and there are stringent controls in place regarding access and use of the data. Decisions on whether DfE releases data to third parties are subject to a strict approval process and based on a detailed assessment of:

- who is requesting the data
- the purpose for which it is required
- the level and sensitivity of data requested: and
- the arrangements in place to store and handle the data

To be granted access to student information, organisations must comply with strict terms and conditions covering the confidentiality and handling of the data, security arrangements and retention and use of the data.

For more information about the department's data sharing process, please visit: https://www.gov.uk/data-protection-how-we-collect-and-share-research-data

For information about which organisations the department has provided student information, (and for which project), please visit the following website: https://www.gov.uk/government/publications/national-student-database-requests-received

To contact DfE: https://www.gov.uk/contact-dfe

Requesting access to your personal data

Under data protection legislation, parents and students have the right to request access to information about them that we hold. To make a request for your personal information, or be given access to your child's educational record, contact Mrs A Hartley, PA to the Headteacher

You also have the right to:

- object to processing of personal data that is likely to cause, or is causing, damage or distress
- prevent processing for the purpose of direct marketing
- object to decisions being taken by automated means
- in certain circumstances, have inaccurate personal data rectified, blocked, erased or destroyed; and
- claim compensation for damages caused by a breach of the Data Protection regulations

If you have a concern about the way we are collecting or using your personal data, we request that you raise your concern with us in the first instance. Alternatively, you can contact the Information Commissioner's Office at https://ico.org.uk/concerns/

Contact

If you would like to discuss anything in this privacy notice, please contact:

- **Steve Bridgman, Deputy Headteacher, data protection officer.**

Data Retention

1. The purpose of the retention schedule

St Benedict's School recognises that the efficient management of its records is necessary to comply with its legal and regulatory obligations and to contribute to the effective overall management of the school. The retention policy lays down the length of time which the record needs to be retained and the action which should be taken when it is of no further administrative use.

Members of staff are expected to manage their current record keeping systems using the retention schedule and to take account of the different kinds of retention periods when they are creating new record keeping systems.

The retention schedule refers to all information, regardless of the media in which they are stored.

2. Safe Disposal of Records

Destruction of records

Where records have been identified for destruction they should be disposed of in an appropriate way. All recor
sensitive policy information should be shredded before disposal (if possible). Any other records should be bu
paper merchant or disposed of in other appropriate ways.

The Freedom of Information Act 2000 requires the school to maintain a list of records which have been
destruction. Members of staff should record at least:

- File reference (or other unique identifier);
- File title (or brief description);
- No of files
- The name of the authorising officer

This could be kept in an Excel spreadsheet or other database format.

Transfer of information

Where lengthy retention periods have been allocated to records, members of staff may wish to consider con
such as microform or digital media. The lifespan of the media and the ability to migrate data where necessary s

3. Maintaining and amending the retention schedule

Where appropriate the retention schedule should be reviewed and amended to include any new record series created and remove any obsolete record series.

4.1 Governors

Basic file description	Data Prot Issues	Statutory Provisions	Retention Period [operational]	Action at the end of the administrative life of the record	
Minutes					
• *Principal set (signed)*	No		Permanent	Retain in school for 6 years from date of meeting	Transfer to Archives
• *Inspection copies*	No		Date of meeting + 3 years	DESTROY [If these minutes contain any sensitive personal information they should be shredded]	
Agendas	No		Date of meeting	DESTROY	
Reports	No		Date of report + 6 years	Retain in school for 6 years from date of meeting	Transfer to Archives [The appropriate archivist will then take a sample for permanent preservation]
Annual Parents' meeting papers	No		Date of meeting + 6 years	Retain in school for 6 years from date of meeting	Transfer to Archives [The appropriate archivist will then take a sample for permanent preservation]
Instruments of Government	No		Permanent	Retain in school whilst school is open	Transfer to Archives when the school has closed
Trusts and Endowments	No		Permanent	Retain in school whilst operationally required	Transfer to Archives
Action Plans	No		Date of action	DESTROY	It may be appropriate to offer to the Archives for a sample to be

4.1 Governors

Basic file description	Data Prot Issues	Statutory Provisions	Retention Period [operational]	Action at the end of the administrative life of the record	
			plan + 3 years		taken if the school has been through a difficult period
Policy documents	No		Expiry of policy	Retain in school whilst policy is operational (this includes if the expired policy is part of a past decision making process)	Transfer to Archives [The appropriate archivist will then take a sample for permanent preservation]
Complaints files	Yes		Date of resolution of complaint + 6 years	Retain in school for the first six years Review for further retention in the case of contentious disputes Destroy routine complaints	
Annual Reports required by the Department for Education and Skills	No	Education (Governors' Annual Reports) (England) (Amendment) Regulations 2002.SI 2002 No 1171	Date of report + 10 years		Transfer to Archives [The appropriate archivist will then take a sample for permanent preservation]
Proposals for schools to become, or be established as Specialist Status schools	No		Current year + 3 years		Transfer to Archives [The appropriate archivist will then take a sample for permanent preservation]

4.2 **Management**

Basic file description	Data Prot Issues	Statutory Provisions	Retention Period [operational]	Action at the end of the administrative life of the record	
Log Books	Yes[1]		Date of last entry in the book + 6 years	Retain in the school for 6 years from the date of the last entry.	Transfer to the Archives
Minutes of the Senior Leadership Team and other internal administrative bodies	Yes[1]		Date of meeting + 5 years	Retain in the school for 5 years from meeting	Transfer to Archives [The appropriate archivist will then take a sample for permanent preservation]
Reports made by the head teacher or the leadership team	Yes[1]		Date of report + 3 years	Retain in the school for 3 years from meeting	Transfer to Archives [The appropriate archivist will then take a sample for permanent preservation]
Records created by head teachers, assistant head teachers, Tutor Team Leaders/Directors of Learning and other members of staff with administrative responsibilities	Yes[1]		Closure of file + 6 years	DESTROY If these records contain sensitive information they should be shredded	
Correspondence created by head teachers, head teachers, assistant head teachers, Tutor Team Leaders/Directors of Learning and other of staff with administrative responsibilities	No		Date of correspondence + 3 years	DESTROY If these records contain sensitive information they should be shredded	

4.2 **Management**

Basic file description	Data Prot Issues	Statutory Provisions	Retention Period [operational]	Action at the end of the administrative life of the record	
Professional development plans	Yes		Closure + 6 years	SHRED	
School improvement plans and self-evaluation	No		Closure + 6 years	Review	Offer to the Archives

4.3 Students

Basic file description	Data Prot Issues	Statutory Provisions	Retention Period [operational]	Action at the end of the administrative life of the record	
Admission Registers	Yes		Date of last entry in the book (or file) + 6 years	Retain in the school for 6 years from the date of the last entry.	Transfer to the Archives
Attendance registers	Yes		Date of register + 3 years	DESTROY [If these records are retained electronically any backup copies should be destroyed at the same time]	
Student record cards	Yes				
• *Secondary*			DOB of the Student + 25 years[2]	SHRED	
Student files	Yes				
• *Secondary*			DOB of the Student + 25 years[3]	SHRED	
Special Educational Needs files, reviews and Individual Education Plans	Yes		DOB of the Student + 25 year[4]	SHRED	

[2] In the case of exclusion it may be appropriate to transfer the record to the Behaviour Service
[3] As above
[4] As above

4.3 Students

Basic file description	Data Prot Issues	Statutory Provisions	Retention Period [operational]	Action at the end of the administrative life of the record	
Letters authorising absence	No		Date of absence + 2 years	SHRED	
Absence analysis			Current year + 6 years	SHRED	
Examination results	Yes				
• *Public*	No		Year of examinations + 6 years	DESTROY	Any certificates left unclaimed should be returned to the appropriate Examination Board
• *Internal examination results*	Yes		Current year + 5 years[5]	DESTROY	
Any other records created in the course of contact with Students	Yes/No		Current year + 3 years	Review at the end of 3 years and either allocate a further retention period or DESTROY	
Statement maintained under The Education Act 1996 - Section 324	Yes	Special Educational Needs and Disability Act 2001 Section 1	DOB + 30 years	DESTROY unless legal action is pending	
Proposed statement or amended statement	Yes	Special Educational Needs and Disability Act 2001 Section 1	DOB + 30 years	DESTROY unless legal action is pending	

[5] If these records are retained on the Student file or in their National Record of Achievement they need only be kept for as long as operationally necessary.

4.3 Students

Basic file description	Data Prot Issues	Statutory Provisions	Retention Period [operational]	Action at the end of the administrative life of the record	
Advice and information to parents regarding educational needs	Yes	Special Educational Needs and Disability Act 2001 Section 2	Closure + 12 years	DESTROY unless legal action is pending	
Accessibility Strategy	Yes	Special Educational Needs and Disability Act 2001 Section 14	Closure + 12 years	DESTROY unless legal action is pending	
Children SEN Files	Yes		Closure + 35 years	DESTROY unless legal action is pending	

4.4 **Curriculum**

Basic file description	Data Prot Issues	Statutory Provisions	Retention Period [operational]	Action at the end of the administrative life of the record	
Curriculum development	No		Current year + 6 years	DESTROY	
Curriculum returns	No		Current year + 3 years	DESTROY	
School syllabus	No		Current year + 1 year	It may be appropriate to review these records at the end of each year and allocate a new retention period or DESTROY	
Schemes of work	No		Current year + 1 year	It may be appropriate to review these records at the end of each year and allocate a new retention period or DESTROY	
Timetable	No		Current year + 1 year	It may be appropriate to review these records at the end of each year and allocate a new retention period or DESTROY	
Class record books	No		Current year + 1 year	It may be appropriate to review these records at the end of each year and allocate a new retention period or DESTROY	
Mark Books	No		Current year + 1 year	It may be appropriate to review these records at the end of each year and allocate a new retention period or DESTROY	
Record of homework set	No		Current year + 1 year	It may be appropriate to review these records at the end of each year and allocate a new retention period or DESTROY	
Students' work	No		Current year + 1 year	It may be appropriate to review these records at the end of each year and allocate a new retention period or DESTROY	

4.4 **Curriculum**

Basic file description	Data Prot Issues	Statutory Provisions	Retention Period [operational]	Action at the end of the administrative life of the record	
Examination results	Yes		Current year + 6 years	DESTROY [These records should be shredded]	
SATS records	Yes		Current year + 6 years	DESTROY [These records should be shredded]	
ASP (Analyse School Performance) reports	Yes		Current year + 6 years	DESTROY [These records should be shredded]	
IDSR (Inspection Data Summary Report)	Yes		Current year + 6 years	DESTROY [These records should be shredded]	
Sixth Form value added records	Yes		Current year + 6 years	DESTROY [These records should be shredded]	

4.5 Personnel

Basic file description	Data Prot Issues	Statutory Provisions	Retention Period [operational]	Action at the end of the administrative life of the record
Timesheets, sick pay	Yes	Financial Regulations	Current year + 6 years	SHRED
Staff Personal files	Yes[6]		Termination + 7 years	SHRED
Interview notes and recruitment records	Yes		Date of interview + 6 months	SHRED
Pre-employment vetting information (including CRB checks)	No	CRB guidelines	Date of check + 6 months	SHRED [by the designates member of staff]
Disciplinary proceedings:	Yes		**Please note that all these retention periods where the warning relates to child protection issues may change in light of any recommendations made by the Bichard Inquiry.**	
• *Oral warning*			Date of warning + 6 months	SHRED If this is placed on a personal file, it must be weeded from the file.
• *written warning – level one*			Date of warning + 6 months	SHRED If this is placed on a personal file, it must be weeded from the file.

[6] These files should be subject to KCC's open file policy where the employees are employed by RECORDS MANAGEMENT SOCIETY OF GREAT BRITAIN as the Local Education Authority.

4.5 Personnel

Basic file description	Data Prot Issues	Statutory Provisions	Retention Period [operational]	Action at the end of the administrative life of the record
• *written warning – level two*			Date of warning + 12 months	SHRED If this is placed on a personal file, it must be weeded from the file.
• *final warning*			Date of warning + 18 months	SHRED If this is placed on a personal file, it must be weeded from the file.
• *case not found*			DESTROY immediately at the conclusion of the case	
Records relating to accident/injury at work	Yes		Date of incident + 12 years	Review at the end of this period. In the case of serious accidents a further retention period will need to be applied
Annual appraisal/assessment records	No		Current year + 5 years	SHRED
Salary cards	Yes		Last date of employment + 85 years	SHRED
Maternity pay records	Yes	Statutory Maternity Pay (General) Regulations 1986 (SI 1986/1960), revised 1999 (SI 1999/567)	Current year, +3yrs	SHRED
Records held under Retirement Benefits Schemes (Information Powers) Regulations 1995	Yes		Current year + 6 years	SHRED

4.6 Health and Safety

Basic file description	Data Prot Issues	Statutory Provisions	Retention Period [operational]	Action at the end of the administrative life of the record	
Accessibility Plans		Disability Discrimination Act	Current year + 6 years	DESTROY	
Accident Reporting		Social Security (Claims and Payments) Regulations 1979 Regulation 25. Social Security Administration Act 1992 Section 8. Limitation Act 1980			
• *Adults*	Yes		Current year + 3 years	SHRED	
• *Children*	Yes		DOB + 25 years[7]	SHRED	
COSHH			Current year + 10 years	Review [where appropriate an additional retention period may be allocated]	
Incident reports	Yes		Current year + 20 years	SHRED	
Policy Statements			Date of expiry + 1 year	DESTROY	

4.6 Health and Safety

Basic file description	Data Prot Issues	Statutory Provisions	Retention Period [operational]	Action at the end of the administrative life of the record	
Risk Assessments			Current year + 3 years	DESTROY	
Process of monitoring of areas where employees and persons are likely to have come in contact with **asbestos**			Last action + 40 years	DESTROY	
Process of monitoring of areas where employees and persons are likely to have come in contact with **radiation**			Last action + 50 years	DESTROY	
Fire Precautions log books			Current year + 6 years	DESTROY	

4.7 Administrative

Basic file description	Data Prot Issues	Statutory Provisions	Retention Period [operational]	Action at the end of the administrative life of the record	
Employer's Liability certificate			Permanent whilst the school is open	DESTROY once the school has closed	
Inventories of equipment and furniture			Current year + 6 years	DESTROY	
General file series			Current year + 5 years	Review to see whether a further retention period is required	Transfer to Archives [The appropriate archivist will then take a sample for permanent preservation]
School brochure/prospectus			Current year + 3 years		Transfer to Archives [The appropriate archivist will then take a sample for permanent preservation]
Circulars (staff/parents/Students)			Current year + 1 year	DESTROY	
Newsletters			Current year + 1 year	Review to see whether a further retention period is required	Transfer to Archives [The appropriate archivist will then take a sample for permanent preservation]
Visitors' book			Current year + 2 years	Review to see whether a further retention period is required	Transfer to Archives [The appropriate archivist will then take a sample for permanent preservation]

4.8 Finance

Basic file description	Data Prot Issues	Statutory Provisions	Retention Period [operational]	Action at the end of the administrative life of the record	
Annual Accounts		Financial Regulations	Current year + 6 years		Offer to the Archives
Loans and grants		Financial Regulations	Date of last payment on loan + 12 years	Review to see whether a further retention period is required	Transfer to Archives [The appropriate archivist will then take a sample for permanent preservation]
Contracts					
• under seal			Contract completion date + 12 years	SHRED	
• under signature			Contract completion date + 6 years	SHRED	
• monitoring records			Current year + 2 years	SHRED	
Copy orders			Current year + 2 years	SHRED	
Budget reports, budget monitoring etc			Current year + 3 years	SHRED	
Invoice, receipts and other records covered by the Financial Regulations		Financial Regulations	Current year + 6 years	SHRED	
Annual Budget and background papers			Current year + 6 years	SHRED	
Order books and requisitions			Current year + 6 years	SHRED	

4.8 Finance

Basic file description	Data Prot Issues	Statutory Provisions	Retention Period [operational]	Action at the end of the administrative life of the record	
Delivery Documentation			Current year + 6 years	SHRED	
Debtors' Records		Limitation Act 1980	Current year + 6 years	SHRED	
School Fund – Cheque books			Current year + 3 years	SHRED	
School Fund – Paying in books			Current year + 6 years	SHRED	
School Fund – Ledger			Current year + 6 years	SHRED	
School Fund – Invoices			Current year + 6 years	SHRED	
School Fund – Receipts			Current year + 6 years	SHRED	
School Fund – Bank statements			Current year + 6 years	SHRED	
School Fund – School Journey books			Current year + 6 years	SHRED	
Applications for free school meals, travel, uniforms etc			Whilst child at school	SHRED	
Student grant applications			Current year + 3 years	SHRED	
Free school meals registers	Yes	Financial Regulations	Current year + 6 years	SHRED	
Petty cash books		Financial Regulations	Current year + 6 years	SHRED	

4.9 Property

Basic file description	Data Prot Issues	Statutory Provisions	Retention Period [operational]	Action at the end of the administrative life of the record	
Title Deeds			Permanent	These should follow the property	Offer to Archives
Plans			Permanent	Retain in school whilst operational then	Offer to Archives
Maintenance and contractors		Financial Regulations	Current year + 6 years	DESTROY	
Leases			Expiry of lease + 6 years	DESTROY	
Lettings			Current year + 3 years	DESTROY	
Burglary, theft and vandalism report forms			Current year + 6 years	SHRED	
Maintenance log books			Last entry + 10 years	DESTROY	
Contractors' Reports			Current year + 6 years	DESTROY	

4.10 LA

Basic file description	Data Prot Issues	Statutory Provisions	Retention Period [operational]	Action at the end of the administrative life of the record	
Secondary transfer sheets (Primary)	Yes		Current year + 2 years	SHRED	

4.10 LA

Basic file description	Data Prot Issues	Statutory Provisions	Retention Period [operational]	Action at the end of the administrative life of the record	
Attendance returns	Yes		Current year + 1 year	DESTROY	
Circulars from LA			Whilst operationally required	Review to see whether a further retention period is required	Transfer to Archives [The appropriate archivist will then take a sample for permanent preservation]

4.11 **DfE**

Basic file description	Data Prot Issues	Statutory Provisions	Retention Period [operational]	Action at the end of the administrative life of the record	
HMI reports			These do not need to be kept any longer		Transfer to Archives [The appropriate archivist will then take a sample for permanent preservation]
OFSTED reports and papers			Replace former report with any new inspection report	Review to see whether a further retention period is required	Transfer to Archives [The appropriate archivist will then take a sample for permanent preservation]
Returns/Census			Current year + 6 years	DESTROY	

4.11 **DfE**

Basic file description	Data Prot Issues	Statutory Provisions	Retention Period [operational]	Action at the end of the administrative life of the record	
Circulars from DfE			Whilst operationally required	Review to see whether a further retention period is required	Transfer to Archives [The appropriate archivist will then take a sample for permanent preservation]

4.12 **Inspira**

Basic file description	Data Prot Issues	Statutory Provisions	Retention Period [operational]	Action at the end of the administrative life of the record	
Service level agreements			Until superseded	SHRED	
Work Experience agreement			DOB of child + 18 years	SHRED	

4.13 **School Meals**

Basic file description	Data Prot Issues	Statutory Provisions	Retention Period [operational]	Action at the end of the administrative life of the record	
Dinner Register			Current year + 3 years	SHRED	
School Meals Summary Sheets			Current year + 3 years	SHRED	

Issued on behalf of the Governing Body by:-

Chair of Governors

10th December 2020
To be reviewed: December 2022

Appendix 1: Personal data breach procedure

This procedure is based on guidance on personal data breaches produced by the ICO.

- On finding or causing a breach, or potential breach, the staff member or data processor must immediately notify the DPO
- The DPO will investigate the report, and determine whether a breach has occurred. To decide, the DPO will consider whether personal data has been accidentally or unlawfully:
    - Lost
    - Stolen
    - Destroyed
    - Altered
    - Disclosed or made available where it should not have been
    - Made available to unauthorised people
- The DPO will alert the headteacher and the chair of governors
- The DPO will make all reasonable efforts to contain and minimise the impact of the breach, assisted by relevant staff members or data processors where necessary. (Actions relevant to specific data types are set out at the end of this procedure)
- The DPO will assess the potential consequences, based on how serious they are, and how likely they are to happen
- The DPO will work out whether the breach must be reported to the ICO. This must be judged on a case-by-case basis. To decide, the DPO will consider whether the breach is likely to negatively affect people's rights and freedoms, and cause them any physical, material or non-material damage (e.g. emotional distress), including through:
    - Loss of control over their data
    - Discrimination
    - Identify theft or fraud
    - Financial loss
    - Unauthorised reversal of pseudonymisation (for example, key-coding)
    - Damage to reputation
    - Loss of confidentiality
    - Any other significant economic or social disadvantage to the individual(s) concerned

  If it's likely that there will be a risk to people's rights and freedoms, the DPO must notify the ICO.
- The DPO will document the decision (either way), in case it is challenged at a later date by the ICO or an individual affected by the breach. Documented decisions are stored on the school's computer system.
- Where the ICO must be notified, the DPO will do this via the 'report a breach' page of the ICO website within 72 hours. As required, the DPO will set out:
    - A description of the nature of the personal data breach including, where possible:
        - The categories and approximate number of individuals concerned
        - The categories and approximate number of personal data records concerned
    - The name and contact details of the DPO
    - A description of the likely consequences of the personal data breach
    - A description of the measures that have been, or will be taken, to deal with the breach and mitigate any possible adverse effects on the individual(s) concerned
- If all the above details are not yet known, the DPO will report as much as they can within 72 hours. The report will explain that there is a delay, the reasons why, and when the DPO expects to have further information. The DPO will submit the remaining information as soon as possible

- The DPO will also assess the risk to individuals, again based on the severity and likelihood of potential or actual impact. If the risk is high, the DPO will promptly inform, in writing, all individuals whose personal data has been breached. This notification will set out:
    - The name and contact details of the DPO
    - A description of the likely consequences of the personal data breach
    - A description of the measures that have been, or will be, taken to deal with the data breach and mitigate any possible adverse effects on the individual(s) concerned
- The DPO will notify any relevant third parties who can help mitigate the loss to individuals – for example, the police, insurers, banks or credit card companies
- The DPO will document each breach, irrespective of whether it is reported to the ICO. For each breach, this record will include the:
    - Facts and cause
    - Effects
    - Action taken to contain it and ensure it does not happen again (such as establishing more robust processes or providing further training for individuals)

  Records of all breaches will be stored on the school's computer system.
- The DPO and headteacher will meet to review what happened and how it can be stopped from happening again. This meeting will happen as soon as reasonably possible

Actions to minimise the impact of data breaches

We will take the actions set out below to mitigate the impact of different types of data breach, focusing especially on breaches involving particularly risky or sensitive information. We will review the effectiveness of these actions and amend them as necessary after any data breach.

Sensitive information being disclosed via email (including safeguarding records)

- *If special category data (sensitive information) is accidentally made available via email to unauthorised individuals, the sender must attempt to recall the email as soon as they become aware of the error*
- *Members of staff who receive personal data sent in error must alert the sender and the DPO as soon as they become aware of the error*
- *If the sender is unavailable or cannot recall the email for any reason, the DPO will ask the ICT department to recall it*
- *In any cases where the recall is unsuccessful, the DPO will contact the relevant unauthorised individuals who received the email, explain that the information was sent in error, and request that those individuals delete the information and do not share, publish, save or replicate it in any way*
- *The DPO will ensure we receive a written response from all the individuals who received the data, confirming that they have complied with this request*
- *The DPO will carry out an internet search to check that the information has not been made public; if it has, we will contact the publisher/website owner or administrator to request that the information is removed from their website and deleted*

Other types of breach that you might want to consider could include:

- *Details of pupil premium interventions for named children being published on the school website*
- *Non-anonymised pupil exam results or staff pay information being shared with governors*
- *A school laptop containing non-encrypted sensitive personal data being stolen or hacked*
- *The school's cashless payment provider being hacked and parents' financial details stolen*

Appendix 2:

General Data Protection Regulation: Information Audit

Please list below *all* student, contact or staff data held by your department (other than that held centrally on SIMS, Milk, SISRA, Office 365). Include any data you may have stored on the school network, at home or on portable devices such as laptops, tablets (iPads etc) and smartphones. If your department shares data with a third party (such as online testing or other software provider), please include these details also. Below are some examples of the data you may have stored – delete these before completing the form..

DEPARTMENT:	

Type of data held **Name, UPN, Date of Birth, Assessment Grade etc**	Where are the data held? **Include details of third-party software companies if relevant**	Is this a secure area?* **YES / NO**	File Type **Third-party extract, paper, Excel, Word etc**	Who has access to the data?	Why are these data needed? **Please state the purpose of the data if they cannot be held on SIMS, Milk, SISRA, Office 365, VLE.**	Data Retention **How long are the data held?**