St Benedict's Catholic High School

Data Protection Policy
2026-2028

Approved by[1]			
Name:	Kayleigh Daniels		
Position:	Chair of Governors		
Signed:			
Version Number: 23		**Date:**	September 2026
Proposed review date[2]:	September 2028		

St Benedict's Catholic High School
1971

REVIEW SHEET

The information in the table below details earlier versions of this document with a brief description of each review and how to distinguish amendments made since the previous version date (if any).

Version Number	Version Description	Date of Revision
1	Original	March 2012
2	Minor changes to Privacy Notices	July 2012
3	Changes Highlighted.	November 2012
4	Reformatted only	February 2014
5	Updated to take account of the DfE model Privacy Notices issued July 2014. NOTE: Appendices C and D have been amalgamated.	July 2014
6	Minor revisions and contact detail changes only to Privacy Notices	July 2015
7	Updated Privacy Notices	December 2016
8	Updated Privacy Notices in line with the GDPR.	October 2017
9	Updated Privacy Notices to reflect DfE revised models released January 2018.	January 2018
10	Major re-write to comply with GDPR	May 2018
11	Updated Privacy Notices to reflect DfE revised models released 16 May 2018 and minor amendment to point 4.7	May 2018
12	Updated - Appendix D reflecting DfE Governor Privacy notice - July 2018	September 2018
13	Updated to include changes to model Privacy Notices made by DfE October 2018	October 2018
14	Updated Privacy Notices to reflect DfE revised models released Dec 2018	December 2018
15	Updated Privacy Notices to reflect DfE revised models released August 2019	August 2019
16	Updates: Section 10.5 (data transfers from UK to EEA after 31 January 2020), Updated S9, new S9.2 & new/updated appendices (to make more specific reference to Covid-19 pandemic related use of data, updated consent form (now named Appendix F), updated model privacy notices Appendices B, C and D & new visitor privacy notice Appendix E, new Appendix G Visitor Record Form (old Appendix F renamed to H because it is landscape!))	September 2020
17	Updated with changes to the Covid-19 isolation period from 14 days to 10 days	December 2020
18	Significant and minor policy updates. Significant updates to Privacy Notices, Section 10.5: Data transfers, new definition of third country, explicit inclusion of volunteers (workforce personal data, their role and training), new reference and link to an example data asset register and breach self-assessment tool, removed almost all of Section 9.2 on Public Health Emergencies, reduced consent options, new SAR form with guidance notes, updated consent form to reflect reduced choice. Also replaced GDPR with UK GDPR and updated links throughout, more clearly defined Information Society Services, more explicitly referenced carers as well as parents.	September 2021
19	Minor changes to terminology, addition of reference to IRMS toolkit for record retention for Academies and the need for schools to have a Cyber Response Plan.	May 2022

20	Updated review sheet. New link to updated Visitor Privacy Notice Poster. Significant updates to terminology reference the Surveillance Camera Code of Practice and Procedures which replaced the CCTV Code (and Procedures). Removed all appendices that are forms or stand-alone guides for ease of updating, use, and distribution. Added more references to signpost staff to specific other policies for more technical or detailed guidance on privacy, data protection, and what to do e.g., to the Online safety Policy for remote education requirements. Added more links to guidance staff can rely on.	September 2022
21	Important update to data retention and destruction (recent court rulings). Links updated to the new KAHub; new unitary authorities, and other resources. Example added to clarify when public bodies can rely on legitimate interests to process personal data. Clarifications on parents etc. taking photos. New referral to the (KAHSC model) Online Safety Policy for information about webcam use.	September 2023
22	New section on generative artificial intelligence (gen-AI) and machine learning. New section on parental consent regarding the use of pupils' original works to train gen-AI models. If a setting has pupils aged 13-17 and they use gen-AI tools to create original schoolwork, the risks and benefits of contributing to global machine learning should be explained to them as part of the computing and online safety curriculum. Parental consent in this regard is about intellectual property and copyright (legal age of consent 18) not data protection (no legal age of consent for data sharing but commonly held to be 13 due to the terms of service of social media platforms). Pupils' opinions about opting out of sharing their work like this, even if parents consent, should be sought in the same way as for publishing their name or photo, due to the potential impact on some children and young people's mental health.	September 2024
23	New: Various new rules to reflect the effects of the Data (Use and Access) Act 2025 (DUAA) e.g., on SARs, privacy, & direct marketing. Section on Complaints. Links to new Government support on AI & free Chartered College of Teaching certified assessment of safe & effective AI use. Updated: Links to IRMS retention guidelines; EU data adequacy decisions end-date; reflect the change to the Information Commissioner instead of ICO	October 2025

Contents

1. Introduction 1
1.1. Policy purpose 1
1.2. Policy scope and definitions 1
2. Roles and Responsibilities 3
3. Data Protection Principles 4
3.1. Conditions for the lawful processing of personal data 5
3.2. Conditions for the lawful processing of special categories of data 6
3.3. Deciding which condition to rely on 7
3.4. Privacy Notices 7
4. Individuals' rights and how we protect them 7
4.1. The right to be informed about the collection and use of their personal data 7
4.2. The right of access to their personal data and relevant supplementary information 8
4.3. The right to rectification if the information held is inaccurate or incomplete 8
4.4. The right to erasure of personal data 8
4.5. The right to restrict the processing of personal data 10
4.6. The right to data portability 10
4.7. The right to object to processing 11
4.8. The right to object to automated decision making and profiling 11
5. Making a Complaint
6. Subject Access Requests 11
7. Data Protection and Privacy by Design 14
7.1. DPIAs 14
8. Training & Awareness 15
9. Publication of Information 15
10. Managing Consent 15
10.1. Consent to use personal data including images and voice recordings 15
10.2. Data sharing during a public health emergency: consent and data retention 17
10.3 Consent for the use of generative artificial intelligence (intellectual property) 15
11. Data Security and Integrity 18
11.1. Classification of data 18
11.2. Organisational and technical security measures 19
11.3. Email 20
11.4. Surveillence Cameras 19
11.5 Generative Artificial Intelligence 19
11.6 Transfers of data outside the UK 20
11.7 Record keeping 20
12. Data Sharing 21

13. Data Retention....21
14. Data Disposal....24
15. Breach Reporting....24
16. Our Obligations to our Data Processors....24

Appendix A - Subject Access Request (SAR) Form
Appendix B - Example School Privacy Notice for Pupils
Appendix C - Example School Privacy Notice for Staff
Appendix D - Example School Privacy Notice for Governors
Appendix E - Example School Privacy Notice for Visitors
Appendix F - Model Parental Consent Form: Trips, Images and Pain Relief
Appendix G - Model Visitor Booking/Record Form (Covid-19)
Appendix H - Data Classifications and Handling Requirements

1. Introduction

The Data Protection Act 2018 provides a legal framework for data protection in the United Kingdom (UK). It incorporates the General Data Protection Regulations (GDPR), the legal framework that sets guidelines for the collection and processing of personal information of individuals within the European Union (EU) and is sometimes referred to as UK GDPR.

UK GDPR significantly updates previous Data Protection law to reflect changes in technology and the way organisations collect and use information about people in the 21st century. It regulates the processing of personal data and gives rights of privacy protection to all living persons.

The Data Use and Access Act 2025 (DUAA) significantly updated the DPA 2018 to allow some direct marketing, broaden the scope of automated decision-making, simplify international transfers, introduce a "stop the clock" provision on Subject Access Requests, empower the Secretary of State to designate new categories of special data, and include an explicit duty to safeguard children by design and requirement for simple cookie consent mechanisms.

In accordance with the DPA, we at St. Benedict's Catholic High School recognise that we collect and process personal data and because we decide how and why we do that, we are *data controllers*. This means that we have legal obligations to people regarding how we handle their data and manage their privacy and we must register as a data controller with the Information Commissioner (IC). Anyone can read the details of our ICO notification by going online to https://ico.org.uk/esdwebpages/search and entering our registration number. Data controllers are normally organisations and not people although our Head teacher is responsible for everything we do day-to-day and we have appointed a Data Protection Officer (DPO).

Our ICO Registration Number is: ZB200003

Our Data Protection Officer is: Stephen Bridgman.

Contact our DPO on 01946 692275 or email them at: steve.bridgman@st-benedicts.cumbria.sch.uk

We recognise that when we process personal data it can involve collecting, recording, organising, storing, altering, retrieving, using, disclosing, restricting, and erasing or destroying it, and there can be risks associated with that processing to the people whose data it is. Failure to adequately protect people's personal information can result in significant, even life-changing harm to some individuals, distress, loss of public trust in us, and legal repercussions including fines and other sanctions.

1.1. Policy purpose

Through this policy we aim to ensure that current and future pupils, staff, volunteers, visitors and partner organisations can feel confident that our school is a safe and secure place to learn or work, or visit and to demonstrate our commitment to protecting the rights and privacy of everyone whose data we handle by setting out:

- our obligations in the context of what we do;
- clear roles, responsibilities, reporting and management structures aimed at protecting people's personal data and their rights;
- clear procedures for handling data to achieve our aim of taking reasonable and proportionate steps to protect people.

1.2. Policy scope and definitions

This policy applies to all governors, trustees, staff, and volunteers who handle or have access to personal data regardless of where they are physically working e.g. at home, at another organisation, on trips, and to all personal information processed by us or on our behalf. This includes the personal information of our data subjects accessed or used by other organisations which work for or with us e.g. Local Authority workers, contractors, consultants, certain service providers like pensions or Disclosure & Barring Service (DBS) umbrella bodies. . It may also include the personal data of other people which pupils acquire through schoolwork tasks or while at school e.g. survey results, class Christmas card lists, and pupils will have some responsibilities in line with their capacity to understand and follow rules.

The following definitions explain a little more about our approach to personal data:

'Data processors' are third party organisations which process data on our behalf. They make no decisions about how and why they do that, they just do what we ask them to within the terms of our contract.

'Data subjects' are the people about whom we hold data, and they fall into several general "categories of person", for example, our workforce and their next of kin; pupils, their next of kin, and other professionals involved with them; our contractors (cleaners, caterers, health & safety, and other service providers); agency and other partner organisation workers (supply or peripatetic teachers, educational psychologists).

'Personal data' is any manually or digitally recorded information relating to a living person (a data subject) which identifies them e.g. a name, an email address, an identification number, location data, an image, an IP address, or one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person and may include facts or opinions about them. Some of this category of personal data will require enhanced security measures such as encryption, password protection and stricter electronic as well as manual access controls e.g. a locked filing cabinet. This will be determined on the basis of a risk assessment of the harm that failing to secure the data might cause e.g. bank details due to the risk of potential fraud; contact information due to potential harassment etc.

'Sensitive personal data' or **'special category data'** includes disability status, sexual orientation, sex life, ethnicity, medical information (both physical and mental health), political, philosophical and religious opinions/beliefs, trade union membership, and details of criminal convictions or allegations. This category of personal data requires enhanced security measures such as encryption, password protection and stricter electronic as well as manual access controls e.g. a locked filing cabinet.

'Pseudonymised personal or sensitive personal data' is information that has been de-personalised but key-coded and it can fall within the scope of the UK GDPR and this policy depending on how difficult it is to attribute the pseudonym to a particular individual.

'Supervisory Authority' is the body that regulates compliance with the GDPR and in the UK this is the ICO.

'third country' is the designation given to a country where there is no privacy and security of data equivalence agreement and transfers of personal data are restricted unless the data is specially protected, or an exception applies.

The UK is a 'third country' to states in the EU GDPR zone (the EU member states plus Norway, Liechtenstein and Iceland) so, unless the UK re-joins the European Free Trade Association (EFTA) and the European Economic Area (EEA), we do not have to be governed by the same rules. The exceptions that apply to the UK are the adequacy decision on transfers under EU GDPR and the adequacy decision on transfers under the Law Enforcement Directive on data transfers between the EU and UK. Both decisions expire in December 2025 and immigration data is specifically excluded.

A 'third country' to the UK, is any state or country worldwide which is not a part of the UK and to which the UK under UK GDPR restricts transfers of personal data unless the personal data is specially protected, or an exception applies. The exceptions that apply to some of these 'third countries' are limited and described in the adequacy decisions the UK has made (see Section 10.5 for more information).

We will make anyone with whom we share the personal data of our data subjects aware of our relevant policy, procedures, and expectations at the outset of sharing.

Any breach of this policy, or of the Regulation itself must be reported to our Data Protection Officer and may need to be reported to the IC as the Supervising Authority for the United Kingdom. The breach could be unlawful and result in legal action or prosecution and regardless of any legal repercussions it may also be actionable under our disciplinary procedures.

This policy will be updated as necessary to reflect improving practice in data management, security, and control and to ensure compliance with any changes to relevant legislation.

Associated policies or documents include:

- Overarching Safeguarding Statement

- Child Protection Policy and procedures
- Online Safety Policy and procedures
- Surveillance Camera Procedures
- Freedom of Information Publication Scheme
- Health and Safety Policy and procedures
- Procedures for Using Pupils' Images
- Behaviour Policy and procedures
- Staff Code of Conduct

2. Roles and Responsibilities

Our responsibilities as a data controller include:

- Analysing and documenting the types of personal data we hold and their uses.
- Identifying our lawful basis for processing personal data.
- Having procedures which support the rights of the individual.
- Ensuring consent procedures are lawful.
- Implementing and reviewing procedures to detect, report, and investigate personal data breaches.
- Storing data in safe and secure ways.
- Assessing risks to individual rights and freedoms should data be compromised.

Staff responsibilities include:

- Understanding their data protection obligations in line with their training and professional duties.
- Checking that their data processing activities comply with our policy and are justified.
- Not using data in any unlawful way.
- Storing data carefully and correctly to avoid breaches of data protection.
- Raising concerns, notifying breaches or errors, and reporting anything suspicious or contradictory to this policy or our legal obligations without delay.

The Data Protection Officer's responsibilities include:

- Keeping governors updated about data protection responsibilities, risks, and issues.
- Reviewing the data protection policy, associated policies, and all relevant procedures regularly.
- Ensure data protection training and advice for all staff and others included in this policy takes place.
- Advising on direct marketing issues such as compliance with the law and our policy; how we deal with queries from target audiences or media outlets; and the wording of data protection statements attached to emails and other marketing copy.
- Answering questions on data protection from staff, governors, and other stakeholders.
- Responding to individuals such as parents, pupils, and employees who want information.
- Approving of any third parties that handle our data and any contracts or agreements regarding data processing.

The TLR Holder's (New Technologies) responsibilities include:

- Reviewing the data protection policy, associated policies, and all relevant procedures regularly.
- Assisting with arranging data protection training and advice for all staff and others included in this policy.
- Checking on any third parties that handle our data and any contracts or agreements regarding data processing

The Senior IT Technician's responsibilities include: (Darren Best)

- Ensuring all systems, services, software, and equipment meet acceptable security standards and can be appropriately filtered and monitored.
- Checking security hardware and software regularly to ensure it is functioning properly and securely.

- Researching relevant third-party services (cloud services, data shredding etc.) that we are considering using.
- Contribute to reviews of the data protection policy, associated policies, and all relevant procedures regularly.
- Assisting with data protection training and advice for all staff and others included in this policy.
- Checking on any third parties that handle our data and any contracts or agreements regarding data processing

3. Data Protection Principles

We understand that as a data controller we are responsible for, and need to be able to demonstrate that we comply with the principles set out in Article 5 of the GDPR which requires that:

a). Personal data shall be processed lawfully, fairly and in a transparent manner in relation to individuals.

We aim to achieve this through carefully considering why we need data before we ask people for it; by publishing our Privacy Notices, implementing them, and reminding people about what the notices says when we ask for data; and by educating our workforce on what they mean for their day-to-day practice.

b). Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.

By keeping our Privacy Notices updated, implementing them, and educating our workforce about what we have and have not agreed to use data for (also in line with requirement a) above), we can ensure we meet this obligation to restrict our processing of personal data. The law does allow us to further process data for archiving purposes in the public interest, or for scientific or historical research purposes or statistical purposes and we have declared that we might do this in our Privacy Notice.

c). Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

We will not seek to collect or process personal data which is not strictly necessary for the reasons we asked to be given it. We keep this in mind when we draft data requests and when irrelevant information is provided we take all reasonable steps to return or erase it.

d). Personal data shall be accurate and, where necessary, kept up to date.

We review and update personal data on a regular basis. It is the responsibility of individuals providing personal data to ensure it is accurate. Individuals should notify us by any reasonable means, but preferably in writing, if their personal data needs to be updated e.g. a change of name or contact details. We will take every reasonable step to ensure that inaccurate personal data (after considering the reasons it is being processed), is erased or rectified without delay, for example, some records are historical and should not be changed.

e). Personal data shall be kept for no longer than is necessary.

We will not retain personal data in a form which allows people to be identified for longer than is necessary to use it for the reasons we asked for it. We employ organisational and technical security measures required by the UK GDPR in order to safeguard the rights and freedoms of individuals, as well as follow strict information transfer guidelines when we need to move data e.g., when a pupil leaves to attend another school. We hold regular reviews of the data we retain and destroy or archive in line with guidance from our Local Authority in the Retention and Disposal Schedule accessible from the Privacy Notice | Cumberland Council and in the IRMS Retention Schedule for schools - Information and Records Management Society.

The law does allow us to retain personal data for archiving purposes in the public interest, or for scientific or historical research purposes or statistical purposes and we have declared that we might do this in our Privacy Notices.

f). Personal data shall be processed in a manner that ensures appropriate security of it.

We understand that our organisational and technical measures to protect data must include protection against unauthorised or unlawful processing and against accidental loss, destruction or damage in the UK, European Union or anywhere else in the world.

We make staff and volunteers aware of their data protection responsibilities and that their duty to preserve confidentiality extends to anywhere that they process the data of our data subjects e.g. at home, on trips etc. and beyond their time of employment with us. See Section 10.2 for more information about the organisational and technological measures we employ to achieve this.

The first principle of data protection is **fair, lawful and transparent processing**, and is the foundation on which everything else is built. We seek to meet the "fair" and "transparent" aspects through our Privacy Notices, and we work hard to ensure that all of the personal data we process meets a condition for lawful processing so that we have a lawful basis to carry it out.

3.1. Conditions for the lawful processing of personal data

To process a piece of personal data we must satisfy at least one condition for the lawful processing of personal data from Article 6 of the GDPR set out in below.

6(1)(a)	Consent of the data subject.
6(1)(b)	Necessary for the performance of a contract with the data subject or to take steps to enter into a contract.
6(1)(c)	Necessary for compliance with a legal obligation.
6(1)(d)	Necessary to protect the vital interests (life) of a data subject or another person.
6(1)(e)	Necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.
6(1)(f)	Necessary for legitimate interests of the controller or a third party, except where such interests are overridden by the interests, rights or freedoms of the data subject (not available to processing carried out by public authorities in the performance of their tasks).

We rely on different conditions for the lawful processing of personal data for different things.

To process the personal data of our workforce and volunteers we generally rely on 6(1)(b) i.e. to employ them and provide training, uniform, pay or expenses etc. Some pieces of data are processed for other reasons. For example, we use their national insurance number for tax purposes relying on 6(1)(c); we hold their next of kin data relying on 6(1)(d); and we use their image relying on 6(1)(f) regarding surveillance cameras and staff/visitor ID badges and sometimes 6(1)(a) e.g., any publishing that is not necessary and we keep them informed about school activities, events, and opportunities relying on 6(1)(f)..

To process the personal data of our pupils. and their relatives or carers we generally rely on 6(1)(e) i.e. to educate them. Some pieces of data are processed for other reasons. For example, we publish pupils' exams/SATs results relying on 6(1)(c) because the law requires us to; we hold their next of kin data relying on 6(1)(d); we process financial information to fulfil contracts e.g., to provide meals; and we use

their image mostly relying on 6(1)(f) but sometimes relying on 6(1)(a) e.g., publishing and we keep them informed about school activities, events, and opportunities relying on 6(1)(f).

We rely on different conditions to process different pieces of the personal data of families e.g. 6(1)(b) for their financial details to provide meals, photographs etc.; and 6(1)(d) for their contact details in case their child is ill. We use the same criteria to process the personal data of other individuals such as contractors or Local Authority workers etc. where it applies and most often using 6(2)(b) to work together nd 6(1)(f) to keep each other informed about school activities.

For more details please see our privacy notices.

In line with provisions in DUAA 2025, we implement a soft opt-in for direct electronic marketing to anyone currently involved with us to keep them up to date. Anyone can ask to opt out at any time using the link that we **must** include in every digital communication of this kind.

3.2. Conditions for the lawful processing of special categories of data

To process a piece of sensitive personal data we must satisfy at least one condition for the lawful processing of special categories of data from Article 9 of the GDPR set out the table below **as well as** one condition from the previous table.

9(2)(a)	Explicit consent of data subject, unless prohibited by EU/National law.
9(2)(b)	Necessary to meet obligations under employment, social security or social protection law, or a collective agreement.
9(2)(c)	Necessary to protect the vital interests (life) of a data subject or another individual where the data subject is physically or legally incapable of consenting.
9(2)(d)	Processing by a not-for-profit body with political, philosophical, religious or trade union aims if it relates only to members/former members (or those in regular contact for those purposes) & there is no disclosure to third parties without consent.
9(2)(e)	Processing relates to personal data already made public by the data subject.
9(2)(f)	For the establishment, exercise or defence of legal claims or court judicial capacity.
9(2)(g)	Substantial public interest under EU/National law proportionate to the aim pursued and which contains appropriate safeguards.
9(2)(h)	For preventative or occupational medicine; assessing work capacity of an employee, medical diagnosis, providing health & social care or treatment or management of healthcare services under EU/National law or contract with a health professional.
9(2)(i)	For public health e.g. protecting against serious cross-border threats to health or ensuring high standards of healthcare & medicinal products or medical devices.

We rely on different conditions for the lawful processing of sensitive personal data for different things.

To process the sensitive personal data of our workforce and volunteers we rely on 9(2)(b) to check their criminal history before employing them; 9(2)(h) to use their health information to protect them at work; 9(2)(a) to share their health information with support services; 9(2)(i) to report on their health to UK Health Security Agency (UKHSA), local Health Protection Team (HPT)or the Health & Safety Executive (HSE) as required; and 9(2)(f) to retain accident and ill-health information in case of a claim for compensation.

To process the sensitive personal data of our pupils we rely on 9(2)(b) in respect of child protection and multi-agency safeguarding work; 9(2)(b) or 9(2)(h) to use their health information to protect them at school; 9(2)(i) to report on their health to UKHSA, local HPTs, or the HSE as required; and 9(2)(f) to retain accident and ill-health information in case of a claim for compensation.

We apply the same criteria to processing the sensitive personal data of families and other individuals such as contractors or Local Authority workers etc. where it applies.

3.3. Deciding which condition to rely on

More than one lawful basis may apply, but we only need **one** basis for each piece of data, and we will rely on what best fits the purpose, not what is easiest. When carrying out a new task or an existing task in a new way, staff should consider the following factors:

- What is the purpose for processing the data?
- Can it reasonably be done in a different way?
- Is there a choice as to whether or not to process the data?
- Who does the processing benefit?
- After selecting the lawful basis, is this the same as the lawful basis the data subject would expect?
- What is the impact of the processing on the individual?
- Are we in a position of power over them?
- Are they a vulnerable person?
- Would they be likely to object to the processing?
- Are we able to stop the processing at any time on request, and have we factored in how to do this?

3.4. Privacy Notices

Our Privacy Notices are an important and necessary way of being transparent and telling governors, parents, pupils, staff, contractors, and visitors what we are doing with their information. To comply with the law it will include:

- Our identity and contact details as the data controller and those of our DPO.
- The purpose of the processing and the lawful basis or bases we are relying on.
- Our, or a third party's legitimate interests in having it.
- The categories of personal data we process.
- Any recipient or categories of recipients of the personal data.
- Details of transfers to UK Government determined "third countries" and the safeguards.
- Retention periods or the criteria used to determine them.
- The existence of each of the data subject's rights.
- The right to withdraw consent at any time, where relevant.
- The right to lodge a complaint with the ICO.
- The sources of personal data and whether they are publicly accessible.
- Whether providing personal data is statutory or contractual and the possible consequences of failing to provide it.
- The existence of any automated decision making, including profiling; how decisions are made, the significance and the consequences.

Our privacy notice relevant to pupils can be found at Appendix B, the one relevant to our workforce and volunteers at Appendix C, the one relevant to our governors at Appendix D, and the one relevant to our visitors at Appendix E. They are also made available on our website, on noticeboards, in communications with parents and staff etc.

4. Individuals' rights and how we protect them

We recognise that all data subjects have "qualified rights" so they are not absolute rights in all circumstances. They are qualified by the rights of other individuals and the legal rights of the data controller or processor to conduct their lawful business.

4.1. The right to be informed about the collection and use of their personal data

Our Privacy Notices seek to provide transparency about our collection of personal data; they are published on our website, pinned to noticeboards, and freely available on request from our office; we

draw people's attention to what they say when we collect data from them; and we regularly review and update the Notices when necessary, particularly if we have changed what we use the data for and before we start using it for the new reason.

4.2. The right of access to their personal data and relevant supplementary information

This includes:

- confirmation that their data is being processed;
- access to their personal data; and
- other supplementary information which largely corresponds to the information we must provide in our Privacy Notices.

Any of our data subjects (or their chosen representative or a person with parental responsibility for them) can make a Subject Access Request (SAR). Please see Section 5 for our procedure on handling SARs.

4.3. The right to rectification if the information held is inaccurate or incomplete

Every individual has a responsibility under UK GDPR to provide accurate data. There is no legal definition of accuracy, but we generally understand it to mean that personal data is inaccurate if it is incorrect or misleading on matters of fact.

The right to rectification will depend on why we asked for the personal data. For example: a person's name should **not** be changed to their new married name on the Single Central Record (SCR) because the SCR is a record of information correct at the time of recruitment and vetting. A note should be added to ensure the SCR record can be matched to the correct living person in case of a vetting query using the married name in future, but the record itself should not be changed.

When we receive a request to change the data we hold, we will take reasonable steps to check that the data is accurate and to rectify it if necessary. This means that the more important it is that the data is accurate, the more effort we will make to correct it. We will take into account arguments and evidence provided by the data subject and anything we have already tried to do to ensure the data is accurate.

We can refuse to comply with a request for rectification if the request is manifestly unfounded or excessive, taking into account whether it is repetitive. We can either request a reasonable fee based on the administrative costs of complying with the request, or we can refuse to deal with the request. We will use ICO guidance and our own information management records to make decisions about this and we will contact the person making the request to inform them of our decision (including any fee payable) and the reasons without undue delay and **within one mon**th. We do not have to comply with the request until we have received the fee.

As a matter of good practice, we will restrict the processing of the personal data in question while we are verifying its accuracy regardless of whether the data subject asked us to as is their right (see Section 4.5).

When we have decided whether the data is accurate or not and whether we will change it or not, we will explain our decision to the individual making the request and inform them of their rights to complain to the ICO. We will also make a record of the request and our response similar to the way we handle SARs e.g. date of receipt, the data subject's name, the name and address of requester *(if different)*, the rectification requested, our decision, and the date we communicated the decision.

4.4. The right to erasure of personal data

Under Article 17 of the GDPR individuals have a new right to have their personal data erased. This is also known as the "right to be forgotten". There are no rules about how a request should be made e.g. verbally, in writing etc. so all staff are trained to recognise someone trying to exercise this right. The right is not absolute and only applies if:

- the personal data is no longer necessary for the reason we originally collected or processed it;
- we are relying on consent as our lawful basis for holding the data, and the individual withdraws their consent;

- we are relying on legitimate interests as our basis for processing, the individual objects to the processing of their data, and there is no overriding legitimate interest to continue e.g., our use of surveillance cameras is an overriding legitimate interest for us in order to prevent and detect crime, not to satisfy our public duty to provide education.
- we are processing the personal data for direct marketing purposes and the individual objects;
- we have processed the personal data unlawfully i.e. in breach of the lawfulness requirement of the 1st principle;
- we have to do it to comply with a legal obligation; or
- we have processed the personal data to offer online "information society services" remotely online directly to a child under the age of 13 e.g., an app, game, social media platform etc. Any such services we currently provide, or broker are necessary for education purposes (or are exempt because they are counselling services) so the right to erasure may not apply, but we are aware of our obligations and will act accordingly. We also work hard to appropriately control children's access to the social media platforms we use to communicate with our community.

We have to give special consideration to any request for erasure if the processing of the data is solely based on consent given by a child, especially any processing of their personal data (usually images) on the internet. This is still the case when the data subject is no longer a child because a child may not have been fully aware of the risks involved in the processing at the time of consent. In some circumstances we might need to give more weight to a request for erasure from a child if their parent has already consented to the use of their data e.g. removing pictures from our school website when a parent has consented but the child whose images they are objects. We will need to do this if we are confident that the child understands their rights and the effects on them of their request. For more information about how we decide whether a child understands please see Section 5 on Subject Access Requests.

Unless it is impossible or disproportionate, we have to tell other organisations about erased data if:

- the personal data we erased has been disclosed by us to others; or
- the personal data has been made public in an online environment (for example on social media, forums or websites).

If we are asked, we should also tell the individual about the other organisations we gave their data to.

The right to erasure does **not** apply if processing is necessary for one of the following reasons:

- to exercise the right of freedom of expression and information;
- to comply with a legal obligation;
- for the performance of a task carried out in the public interest or in the exercise of official authority;
- for archiving purposes in the public interest, scientific research, historical research or statistical purposes where erasure is likely to make achievement of that processing impossible or disproportionately difficult; or
- for the establishment, exercise or defence of legal claims.

There are also two circumstances when the right to erasure does **not** apply to special category data:

- if the processing is necessary for public health purposes in the public interest; or
- if the processing is necessary for the purposes of preventative or occupational medicine.

When we receive a request to erase data, we will take reasonable steps to check the identity of the requester and that they have the right to make the request before considering it.

We can refuse to comply with a request when an exemption applies, or when the request is manifestly unfounded or excessive. We can either request a reasonable fee based on the administrative costs of complying with the request, or we can refuse to deal with the request. We will use ICO guidance and our own information management records to make decisions about this and we will contact the person making the request to inform them of our decision (including any fee payable) and the reasons without undue delay and **within one month**. We do not have to comply with the request until we have received the fee.

When we have decided whether we can erase the data we will explain our decision to the individual making the request and inform them of their rights to complain to the ICO. We will also make a record of

the request and our response similar to the way we handle SARs e.g. date and manner of request (verbally to class teacher, a note handed to reception etc.), the data subject's name, the name and address of requester *(if different)*, the erasure requested, our decision, and the date we communicated the decision.

4.5. The right to restrict the processing of personal data

Under Article 18 of the GDPR individuals have the right to limit the way we use their data if they have a particular reason for wanting to, and this is an alternative to erasing it. They may have issues with the content of the information or how we have processed it. In most cases we will not be required to restrict an individual's personal data indefinitely but will need to have the restriction in place for a certain period of time. The right is not absolute and only applies if:

- the individual contests the accuracy of their personal data and we are verifying it;
- the data has been unlawfully processed i.e. in breach of the 1st principle, and the individual doesn't want it erased;
- we no longer need the personal data but the individual needs us to keep it in order to establish, exercise or defend a legal claim; or
- the individual has objected to us processing their data under Article 21(1), and we are considering whether our legitimate grounds override those of the individual.

We use the most appropriate method applicable at the time to restrict processing including:

- temporarily moving the data to another processing system;
- making the data unavailable to users; or
- temporarily removing published data from a website.

While a restriction is in place we will not do anything with data except store it unless:

- we have the individual's consent;
- it is for the establishment, exercise or defence of legal claims;
- it is for the protection of the rights of another person; or
- it is for reasons of important public interest.

If we have disclosed the restricted data to another organisation we will tell them about the restriction in the same way as if it were inaccurate data unless this proves impossible or involves disproportionate effort. If asked to, we will also inform the individual about these recipients.

We can lift the restriction when we have decided that the issues are resolved i.e. the data is accurate or our legitimate grounds override the individuals' and we will inform the individual and include our reasons before we lift it. We will also tell them about their right to make a complaint to the ICO.

We can refuse to comply with a request when the request is manifestly unfounded or excessive. We can either request a reasonable fee based on the administrative costs of complying with the request, or we can refuse to deal with the request. We will use ICO guidance and our own information management records to make decisions about this and we will contact the person making the request to inform them of our decision (including any fee payable) and the reasons without undue delay. We do not have to comply with the request until we have received the fee.

4.6. The right to data portability

The right to data portability only applies when all 3 of the following conditions are met:

- the individual has provided the personal data;
- the processing is based on the individual's consent or for performance of a contract; **and**
- processing is carried out by automated means.

We do not currently hold any qualifying data, but we are aware of our legal obligations and will follow IC guidance, reviewing our procedures if we automate any processing.

4.7. The right to object to processing

Individuals must have an objection on "grounds relating to his or her particular situation" and we must stop processing the personal data unless:

- we can demonstrate compelling legitimate grounds for the processing, which override the interests, rights and freedoms of the individual; or
- the processing is for the establishment, exercise or defence of legal claims.

We will:

- inform individuals of their right to object "at the point of first communication" and in our privacy notices, explicitly bringing the right to their attention clearly and separately from any other information;
- stop processing personal data for *direct marketing purposes* as soon as we receive an objection because there are no exemptions or grounds to refuse; and
- deal with an objection to processing for *direct marketing* at any time and free of charge.

An individual can object to processing for research purposes on "grounds relating to his or her particular situation" unless processing is necessary for the performance of a public interest task.

We carry out some processing of personal data securely in encrypted online systems e.g. our visits approval system, responding to DfE data demands online, and any individual can object to our online processing by contacting us at steve.bridgman@st-benedicts.cumbria.sch.uk

4.8. The right to object to automated decision making and profiling

We do not currently process any personal data through automated decision making or profiling, although we occasionally work with organisations that do e.g., exam boards that use multiple choice exam formats.

We are aware of our legal obligations and will follow IC guidance, reviewing our policy and procedures if this changes in the future.

5. Making a Complaint

For ease of handling and to help ensure legal compliance, consider keeping complaints about the use of personal data separate from all other kinds of complaints by developing an online complaint form modelled on future IC guidance].

Anyone whose data we process has the right to complain to us if they think we have not upheld their legal rights, and we have a duty to respond appropriately in a reasonable timeframe.

We treat complaints about the use of personal data in the same as any other complaint. It can be brought to the attention of a member of staff informally to try to resolve the issue, in person or another way. If still unhappy, the ordinary Complaints Procedure [insert link to school complaints procedure] should be followed, with concerns being put in writing to the Head teacher.

It is the responsibility of [insert role] to ensure that, when informal resolution of a complaint about the use of personal data has not been possible, complainants are asked to put their complaint in writing [insert how e.g., to name/role & contact details and are referred to IC guidance on How to make a data protection complaint to an organisation | IC to help them explain it. Their attention must be drawn to the end of the guidance which explains how to complain to the IC if they are not satisfied with our response.

All formal and informal complaints involving personal data, no matter how minor or easily solved, must be reported to the DPO for monitoring purposes. The DPO will decide if it should be recorded as a possible breach of GDPR for internal risk assessment and training purposes or if significant harm has arisen and it should be reported to the IC.

6. Subject Access Requests

Every individual who is our data subject has the right to access their personal data so that they are aware of and can verify the lawfulness of the processing, including children of any age who understand what they are requesting.

A data subject is only entitled to such confirmation, personal data and other information as we, the controller, are able to provide based on a **reasonable and proportionate search** for it. This change to data protection legislation applies retroactively to any SAR that has not been processed to conclusion, regardless of whether it was submitted before 19 June 2025 when this 'proportionate and reasonable search' condition was codified into law.

These rights do not automatically override the rights of any other individual who might be identified by our response to a request, so we will make a decision on what information to disclose by balancing the data subject's right of access against any other individuals' rights in respect of their own personal data. We will use the latest IC guidance on SARs to help us make decisions.

The data subject or the person acting on their behalf must make a SAR in writing and we provide a form at Appendix A to help people do this. There is no requirement to use our form, but it can speed up the process by helping the people making requests to provide us with the kind of information we need to comply. We will also make any reasonable adjustment for disabled people who may be unable to make their SAR or receive information in writing e.g. accepting a verbal request, providing a braille response etc. Relevant staff are trained to recognise a SAR even when it does not include the words "subject access", or refer to the applicable legislation, including where the wrong legislation is quoted i.e. often the Freedom of Information Act.

When we receive a SAR it will be entered in the Subject Access Request log book, including the date of receipt, the data subject's name, the name and address of requester *(if different)*, the type of data requested (e.g. pupil record, personnel record), whether there is enough information to respond appropriately (and the immediate action taken to seek more if not), and the expected date for providing the information.

We aim to provide information without delay and at the latest **within one month** of receipt of the request. For example: if we receive a SAR on the 10th of the month we will respond by the 10th of the following month. We will seek to extend this response period by up to the two further months which the law allows where requests are complex or numerous. If this is the case, we will inform the individual within one month of the receipt of the request and explain why the extension is necessary.

Because we process large amount of data about individuals, we may also "stop the clock" on our response to a SAR if we need to ask the requestor to specify the information or processing activities that they want. The time limit for responding to the request will be paused until we receive clarification.

We will not seek clarification on a blanket basis. We will seek it if:

- it is genuinely required in order to respond to the SAR; and
- we process a large amount of information about the individual.

We can request clarification as long as we are satisfied that we hold a large amount of information, *and* it is not clear what information the individual is requesting. We are not required to seek clarification and can choose to follow IC guidance How do we find and retrieve the relevant information? | IC and perform a reasonable search instead.

When we receive a SAR during the longer periods when school is not operational, especially over the summer holiday, we reserve the right to decide that the request is complex due to its timing and the lack of necessary resources available to carry out the request. If so, we will write to the requestor within 1 month of receiving the request (including during all holiday periods) advising of our decision to treat their request as complex and why, and to reasonably extend our response period by up to two further months.

SARs made by pupils will be processed in the same way as any other SAR and the information will be provided to the child regardless of their age unless it is clear that they do not understand their rights. If we are sure that the pupil **does not** understand the SAR and their rights, we will refer the matter to parents, comply if they agree, and provide the information to parents.

SARs made by people on behalf of children they hold parental responsibility for will be processed in the same way as any other SAR while recognising that they do not own the data they are requesting. If we are confident that the pupil whose data it is **does** understand the SAR and their rights, then we will respond to the child rather than the parent, even where the parent was the one who made the request.

In making our decision we will take the following, amongst other things, into account:

- the child's level of maturity and their ability to make decisions like this;
- the nature of the personal data;
- any court orders relating to parental access or responsibility that may apply;
- any duty of confidence owed to the child or young person (including information about any counselling or other service being offered directly to the child);
- any consequences of allowing those with parental responsibility access to the child's or young person's information (particularly important if there have been allegations of abuse or ill treatment);
- any detriment to the child or young person if individuals with parental responsibility cannot access this information; and
- any views the child or young person has on whether their parents should have access to information about them.

If the information requested by a parent in a SAR relates to the 'educational record' of a pupil, in accordance with *'The Education (Pupil Information) (England) Regulations 2005'*, we will make a pupil's educational record available for inspection by the parent, free of charge, **within fifteen school days** of receipt of the parent's written request for access. This cannot include any information that we could not lawfully disclose to the pupil themselves. If parents request a copy to keep, we can charge the administrative costs of supplying one.

If the information requested in a SAR does **not** relate to the 'educational record' of a pupil, we will provide a copy of the information free of charge **unless** the request is manifestly unfounded or excessive, particularly if it is repetitive. This fee may vary and will be based only on the administrative cost of providing the information. We will use ICO guidance and our own information management records to make decisions about this.

We must verify the identity of the person making the request, using "reasonable means". If the person making the request is not the data subject, we must also verify their right to make such requests on behalf of the data subject e.g. their authority to act or their parental responsibility for a child. In cases where a child is competent to make their own request, information will be provided to the child and not to the parent. We will use ICO guidance and our knowledge of the capability of our pupils as described above to make decisions about this.

If the request is made electronically, we will provide the information in a commonly used electronic format.

If we are asked for a large quantity of information about an individual, we can ask the individual to be more specific about the information they want. This is not because we are exempt from providing large amounts of data, this is so we can consider whether the request is manifestly unfounded or excessive.

If we are asked for information that a data processor we work with holds on our behalf, we will ask our data processor to provide it to us so that we can comply with the SAR. This is because we are the data controller and it is our responsibility. We have written contracts in place with all of our data processors to help us do this.

A Subject Access Request should be made in writing to: Stephen Bridgman, Deputy Headteacher at St Benedict's Catholic High School, Red Lonning, Whitehaven, Cumbria, CA28 8UG – steve.bridgman@st-benedicts.cumbria.sch.uk.

7. Data Protection and Privacy by Design

Data protection and privacy by design is an approach to projects and tasks that promotes privacy and data protection compliance from the start and is a clear legal requirement of us. This is not just about the strategic decisions we make building new IT systems for storing or accessing personal data and developing policy or strategies that have privacy implications. It is also about collecting or sharing data in a new way or using data for new purposes.

Our aim is to minimise privacy risks and build trust so all staff will have a central role to play in keeping what we do compliant. When handling data in a different way staff are trained to first consider the impact of what they are doing and how they are doing it in relation to data protection and privacy, with the ten questions in Section 3.3 playing an important part in the process. This could be as simple as ensuring consent forms containing sensitive personal data are not carried in a clear folder on a trip, or as complex as thoroughly vetting an overseas data transfer service when a pupil leaves us to attend a school outside the European Economic Area (EEA).

We use the ICO guidance on Data Protection Impact Assessments (DPIAs) as an integral part of our approach to data protection and privacy by design. We also consult our DPO at the outset of any new data project.

7.1. DPIAs

We understand that we have a legal obligation to do a Data Protection Impact Assessment (DPIA) before carrying out processing likely to result in a high risk to individuals' interests especially children under DUAA 2025. We will use the IC template to help us get this right. When it involves surveillance cameras, we will use the government guidance and template, Data protection impact assessments for surveillance cameras. If our DPIA identifies a high risk which we cannot mitigate, we must consult the ICO before proceeding.

A DPIA is a process to systematically analyse our processing and help us identify and minimise data protection risks. It is meant to:

- describe the processing and our purposes;
- assess the necessity and proportionality of what we are planning;
- identify and assess risks to individuals; and
- identify any measures to mitigate those risks and protect the data.

It does not have to eradicate the risk but should help to minimise risks and consider whether or not they are justified. We will need to do a DPIA if we plan to:

- use new technologies;
- use profiling or special category data to decide on access to services;
- profile individuals on a large scale;
- process biometric or genetic data;
- match data or combine datasets from different sources;
- collect personal data from a source other than the individual without providing them with a privacy notice ('invisible processing');
- track individuals' location or behaviour;
- profile children or target services at them; or
- process data that might endanger the individual's physical health or safety in the event of a security breach.

All staff have a responsibility to identify when their activities around data imply the need for a DPIA. This could be doing an entirely new task with data, or it could be changing the way a well-established task is being done. DPIAs should be reported to the DPO and will be conducted by the Senior IT technician and/or the TLR holder (New Technologies).

8. Training & Awareness

During their induction, all staff and volunteers will receive suitable training in their responsibilities for data protection in their work or volunteering, and the relevant procedures. This will be supplemented with staff briefings, inset training, and other methods of updating staff and volunteers as necessary e.g. briefing emails, notices etc.

This policy is available to all staff and volunteers in hard copy [Kept in the HR office] and digital copy on the staff network [kept on staff resources drive]. It can also be provided to others on request. This policy will be updated regularly in line with changes in practice or clarifications required after applying it to resolve data protection issues.

Anyone can seek general data handling guidance from the ICO on their website https://ico.org.uk.

Day-to-day support and guidance for staff is available from the DPO. Any other category of person wanting help with a data protection issue e.g. contractors, parents etc. can also contact Darren Best who might be able to help but is not the DPO or are free to contact our DPO using the published contact details.

9. Publication of Information

At times we publish information which includes personal data, for example:

- internal telephone directory,
- event information,
- staff information,
- lists of students in a team.

Other things we publish can be subject to an individual's consent and we will seek it as required and consider all reasonable requests to correct, erase or restrict data processing in line with our legal obligations.

10. Managing Consent

We only need one lawful reason to process personal and special category data and the law provides us with 6 reasons to choose from for personal data (see Section 3.1) and 9 reasons for sensitive personal data (see Section 3.2). This means it is extremely rare for us to have to rely solely on consent as our *only* lawful basis for processing.

When we do need consent and we ask for it, we will include the following information in our request:

- the name of our school;
- the name of any third party controllers who will rely on the consent;
- why we want the data;
- what we will do with it; and
- that individuals can withdraw consent at any time.

People will be asked to actively indicate their consent in words and if there are different options, these will be made clear e.g. consent for a child to participate in an event being clearly separate from any consent to use images of them taken at the event (if no blanket/lasting images consent is already held).

There is no set time limit for consent. How long it lasts depends on the context and what we have told people in our Privacy Notices or other communications. We review and refresh consents as appropriate.

Genuine consent should put individuals in control, build trust and engagement, and enhance our reputation so, when we do rely on it, we need to keep a record that helps show it was freely given e.g. who consented, when, how, and what they were told.

10.1. Consent to use personal data including images and voice recordings

We *do not* need parental consent to process any personal data including image or voice recordings made for the purposes of education e.g., video of a Performance Assessment for a GSCE examination in PE in a

sport or activity where live moderation is not possible by the school or other Assessment Centre.. Using names, image and voice recordings of children in their work and in displays inside school, is a fundamental part of their education, personal development and how we celebrate them. This does not affect the statutory rights of individuals as set out in Section 4. Anyone can raise any concern with any member of staff about our use of their or their child's data at any time and we are obliged to ensure their rights are upheld where we have no lawful reason to refuse.

We *may* need parental consent to use personal data including image and voice recordings for other reasons such as marketing or self-promotion in publications and on websites or social media platforms directly managed by us or, with our permission, by others associated with us and may include pictures of living people that have been drawn by children. Images that might cause embarrassment or distress will not be used nor will image or voice recordings of children be associated with materials or issues that are considered sensitive. Anyone with parental responsibility for a child can ask to see any images that we hold of them at any time. This does not include images recorded on the School surveillance systems which may include other children.

There is no legally binding age of consent in the UK with regard to the use of an individual's own data, including their image or voice, except when providing an Information Society Service (ISS) directly to a child online and solely on the basis of their consent(which is aged 13). We do not currently offer any ISS and have no plans to. This means that any child of any age can assert their data rights or consent to the use of their data under the law, providing we are sure that they understand their rights and the implications of their consent. For more information about how we make decisions about a child's competence to consent or withdraw consent that their parents have previously provided, please see Section 6 on SARs

Photography, audio recording or filming will only take place at school or school events with the permission of the Head teacher, and under appropriate supervision.

Regardless of who is publishing data, and that includes us, our policy is that children will only be named if there is a particular reason to do so e.g. they have won a prize, and no other personal details will be published or given out. If names will, or might, be published e.g. in a newspaper article, we will check that parents understand the potential implications and consent to the use of names at that time and before the publishing happens. The news media will often require a child's full name before they will publish an image and our policy is to resist this wherever possible and if we fail, we will take steps to ensure that parents are aware that all of the details will be available in local or national newspapers and worldwide online.

We allow parents, carers, and other invited visitors to take images of children at school functions, but we reserve the right to enforce special restrictions on a case-by-case basis.

We explain the rules in writing in event information beforehand, at events with appropriate signage when necessary and an announcement at the start, and we will take reasonable steps to enforce it.

Rules may vary between events but will always include:

- Where photography and filming is permitted or not permitted.
- That photography and filming is permitted for strictly personal and private use only, that everyone has a responsibility to ensure images they keep, and share, are appropriate, and that they should not be shared on social media without the express permission of everyone in them (and/or their parents or carers).
- That those who want to take pictures or film must not disturb other people's view or enjoyment.

A reminder about our Behaviour Policy and Online Safety Policy which says that no child or adult associated with us in any way should ever upload or post online any content (pictures, audio, video, or text) that could upset, offend, or threaten the safety of any member of our community or bring us into disrepute..

Our policy on requesting consent is to ask once when a child starts their career with us for separate general consents to use image and/or voice recordings:

a) By publishing them on our website or in other print or online media which we directly control, or

b) By allowing carefully selected third party organisations such as local media outlets to publish them.

We use the form at Appendix E to seek consent and we remind parents and children regularly that they can change or withdraw their consent at any time.

When a child understands their right of consent and its full effects and there are no reasons why their name, image or voice must be protected, we can prioritise the consent of a child over parental consent where they are different. We are more likely to decide not to use images etc. when a child objects and their parent does not than vice versa, but our overriding priority will always be to act in the child's best interests.

Staff are expected to make themselves aware of any guidance we use from the ICO, our local authority, Local Safeguarding Children Partnership, or governors and our competent advisors e.g., KAHSC Safety Series: G21 The Use of Images Working with Children, and to apply the principles in all use of image and voice recordings.

10.2. Data sharing during a public health emergency: consent and data retention

In line with our statutory duties, we require anyone who comes into close contact with our pupils. staff, buildings, or equipment (including our staff and pupils) to share with us necessary personal data to give to an organisation authorised by a relevant public health authority so they can take action to protect public health. We do not need consent for this and in a public health emergency this is no different to our normal practice when we are required to report that staff or pupils have contracted a notifiable disease like meningitis or measles, or if we have a food poisoning incident on our premises.

10.3. Consent for the use of generative artificial intelligence (intellectual property)

Most generative artificial intelligence (AI) tools will use the inputs submitted by users to further train and refine their models.

However, pupils own the intellectual property (IP) rights to original content they create. Original content is likely to include anything that shows working out or is beyond answers to multiple choice questions. Intellectual property can only be used to train AI if there is consent from the rights holder or an exemption to copyright applies.

Some tools allow users to opt out of inputs being used to train the models.

Staff training includes that, as a school, we must not allow or cause pupils' original work (content) to be used to train generative AI models unless we hold appropriate consent or exemption to copyright. Without this, staff are responsible for ensuring that, every time they input pupil's original work or allow pupils aged 13 or over to use AI tools, they have opted out of the inputs being used to train the AI models.

Most generative AI tools have terms of service that include a minimum age of 13 years for users but also requires all users aged 13-17 to have the consent of their parent or legal guardian to use them.

This means that pupils under the age of 13 must not use these tools at all and that staff must not input pupils' original work into these tools, unless they opt out of allowing its use for training the AI models, if they don't have evidence that parents have consented to this use of their child's intellectual property. Consent to opt in to sharing pupils' original work to train AI models must be an additional question separate from whether parents consent to their child's original work being input into generative AI tools.

Pupils aged 13-17 can be allowed to use generative AI if their parents consent by indicating their acceptance of the terms of service, and separately, whether they agree to their child's original work being shared to train the AI models being used.

Students aged 18 and over are legal adults and can provide their own consent instead of seeking parental consent. However, we treat all Y13 students equally and have an expectation that their parents or carers will continue to provide the same engagement and parental support to their 18+ year olds as we expected when they were younger i.e., completing consent forms or slips, providing home emergency contacts.

Currently, this school supports limited analytical, administrative and educational use of open AI services such as ChatGPT & DALL-E and Google AI to reduce staff workloads and enhance learning.

Parents of pupils whose original content will be input into a generative AI tool must be sent links to the tool terms of service beforehand e.g. EU terms of use | OpenAI and Google Terms of Service – Privacy & Terms – Google. We will ask them to read these Terms with their child to ensure they understand and agree to them. Parents who receive this information are expected to respond confirming whether they consent to original work by their child aged 12 or under being input into a generative AI tool and/or to their child aged 13+ inputting their own original work into a tool and additionally whether they consent to their child's original work being used to train AI models.

We will take steps to explain to all pupils when relevant, in age/developmental stage appropriate ways, the function and risks of using their original content (and potentially their personal data if they used it to make their content) to contribute to global machine learning. We may not explicitly ask pupils for their consent on issues of intellectual property but they will be taught about online safety and that their opinion of what will happen to their original work or to their personal data matters. An agreement to use their intellectual property from anyone aged 13-17 can *never* override a parent's refusal to consent, but if a parent agrees and their child doesn't, we might decide *not* to use their child's original work. This is because we may need to be sensitive to issues around low self-esteem and anxiety or other mental health issues that can become worse when a pupil feels they lack control over decisions that they feel impact them negatively.

Exemptions to copyright are limited, and if there are any concerns about whether we are acting within the law, current DfE advice suggests we may wish to seek legal advice. This means that all questions or concerns about our use of generative AI should be treated seriously and directed to the Deputy Headteacher

11. Data Security and Integrity

Article 5(1)(f) of the GDPR concerns the 'integrity and confidentiality' of personal data. It says that personal data shall be: "Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures".

The security measures we put in place seek to ensure that the data:

- can be accessed, altered, disclosed or deleted only by those we have authorised to do so and that those people only act within the scope of the authority we give them;
- is accurate and complete in relation to why we are processing it; and
- remains accessible and usable, i.e. if personal data is accidentally lost, altered or destroyed, we should be able to recover it and prevent any damage or distress to individuals.

All staff and any others who process the personal data of our data subjects are expected to work to the same principles we do at all times.

So that immediate responses and actions can be implemented in the event of a cyber-attack on our IT systems, we will have a Cyber Response Plan in place which is regularly reviewed.

The plan covers all essential and critical IT infrastructure, systems, and networks, and will ensure that communications can be quickly established whilst activating cyber recovery. We take steps to ensure that the plan is well communicated and readily available to those with a role in it.

11.1. Classification of data

We carry out regular data audits to identify data that we control and the risks to every kind of processing we do to that data, and we keep a record to help us deal with any issues or requests. As part of this systematic approach we operate 3 levels of data classification to ensure the appropriate security measures can be taken to keep the data safe:

- **Public:** Information that does not require protection and is considered "open and unclassified" and which may be seen by anyone whether directly linked with school or not. Information is likely to already exist in the public domain e.g. the information the DfE publishes about our governors/ trustees on the Get Information About Schools public database online.

- **Confidential:** Information that, if disclosed inappropriately, may result in minor reputational or financial damage to the school or may result in a minor privacy breach for an individual. Information that should only be available to sub-groups of school staff who need the information to carry out their roles.
- **Sensitive:** Information that has the potential to cause serious damage or distress to individuals or serious damage to the school's interests if disclosed inappropriately. Information which is sensitive in some way because it might be sensitive personal data, commercially sensitive, legally privileged or under embargo. This information should only be available to a small tightly restricted group of authorised users.

The appropriate marking of data as to its classification is an operational decision on a case-by-case basis. Most of our data held in electronic databases is classified automatically by the information management systems that hold it. Information that is transferred e.g. emailed, posted, moved to an archive etc. must be appropriate classified and marked to ensure it will be treated properly.

Appendix H sets out some of our specific data security expectations at each different level of data classification and we share it with staff and others who have legal obligation to us when they process data that we control.

All data classifications are reviewed at the point of entry into our archive. All archived data is appropriately labelled with:

- the final data classification;
- any specific restrictions i.e. not to be released to named parent under court order;
- how the data is to be destroyed e.g. incineration, cross-cut shredding, shredding, or electronic data scrubbing/shredding;
- when the data is to be destroyed.

Staff responsible for archiving are trained to assess and manage any increasing risks that can arise as data about one person is aggregated.

11.2. Organisational and technical security measures

The main organisational and technical measures we employ include:

- Appropriate physical security measures for the site, buildings, restricted areas and restricted storage containers including locks, deadlocks, restricted access keys including electronic keys and alarms
- Appropriate physical access and security procedures including limiting access to areas or stores to certain key holders, and procedures to welcome visitors aimed at preventing unauthorised access e.g. visitors' badges, signing in/out, whether a visitor can only access certain areas while accompanied etc.
- Ensuring unauthorised personnel cannot see documents or screens which might display personal data e.g. open registers and visitor's books, emails, CCTV monitors.
- Suitable contracts of employment or technology access agreements for pupils, visitors and others aimed at ensuring the proper use of personal data and maintenance of confidentiality.
- Appropriate storage arrangements that avoid physical risks (flood, fire etc.), loss (lost devices, accidental destruction etc.) or electronic degradation (corruption caused by electricity or magnetism, new software unable to read files created using old software etc.).
- Appropriate technological or procedural security measures including:
    - The installation of appropriate security software (including for virus and malware checking) on all devices used to process personal data, instructions on how to use it properly, and the requirement on all data users to adequately secure devices i.e. carrying portable devices securely and activating an encrypted screen lock when leaving a device unattended even for a minute.
    - Restricting access to school devices containing personal data to employees and specially authorised volunteers, visitors or service providers. Staff using a work device off-site must take steps to secure their work device from use by anyone else including family.

- Enforcing our strict protocol on the use of personal devices to process personal data obtained at work, including a requirement for secure remote access to school systems (See Online Safety Policy, Acceptable Use of IT Policy/Agreement, Staff Code of Conduct);
- Restricting the number of people who can access certain data by limiting online logins, protecting parts of our network to hide them from unauthorised users, and by having procedures in place to designate authorised users and give only them the proper access;
- Enforcing our strict password protocol for access to any personal data whether it is online, on a device, or being transferred somewhere e.g. email containing confidential information must include "confidential" in the subject bar. Documents sent electronically must be password protected. Portable memory devices must be encrypted / password protected. All staff who use Password Managers are required to apply the best practice guidance blog from the National Cyber Security Centre (NCSC).
- Having appropriate data recovery arrangements in place to avoid accidental loss of data or password sharing i.e. so when someone is unavailable to provide access to data, with the proper authorisation their access can be reset and the data still obtained in their absence.
- Appropriate marking or designating of data as private or confidential or sensitive to ensure it is treated accordingly e.g. not printed to a publicly accessible printer.
- Adherence to strict controls on the transfer of data i.e. only as authorised and agreed via encrypted email or portable device, secure websites, password protected files, properly addressed and if necessary fully tracked postal packages, delivery by hand etc.
- Secure methods of disposal for both paper and electronic data shredding.
- Clear policies and procedures for the appropriate archiving and automatic backing up of necessary data including off-site e.g. essential data identified in the Emergency Preparedness Plan to ensure business continuity.
- Clear and binding contracts with our data processors such as our health & safety provider and people who we jointly control data with such as the outdoor adventure centres we go on residential trips to.

All enquiries about the policies and procedures that should be followed and how data should be protected or destroyed can be addressed to the DPO, TLR holder (New Technologies), or the Senior IT technician.

The consequences of getting data security wrong can be very serious for our most vulnerable data subjects and breaches of data protection may be subject to disciplinary action and further subject to legal action or criminal prosecution.

11.3. Email

All staff are expected to adhere to the good practice around the use of email set out in the current Information and Records Management Society "Schools Toolkit' understanding their role and responsibilities with regard to:

- the 8 things they must know about email including that it is not always a secure medium to send confidential information by, that email is disclosable under the Freedom of Information Act 2000, that any employer has a right to monitor the use of email under the Regulation of Investigatory Powers Act 2000, and that email is one of the most common causes of stress in the work-place;
- creating and sending email;
- sending attachments;
- using disclaimers;
- managing received e-mails; and
- retaining emails.

Others who have legal obligations to us because they process data we control will be made aware of our email protocols as necessary.

All staff are required to use the authorised email disclaimer as follows:

Disclaimer: *This e-mail contains confidential information (which may also be legally privileged) and is intended solely for the use of the intended named recipient. If you are not the intended*

recipient you should not disclose, copy, distribute or retain any part of this message or its attachments. If you have received this message in error, please notify the originator immediately and delete this email from your system. Any views or opinions expressed are solely those of the original author. The sender gives no representation or guarantee with respect to the integrity of any emails or attached files and the recipient should check the integrity of and scan this email and any attached files for viruses prior to opening. E-mails and attachments may be encrypted to meet the General Data Protection Regulation (GDPR). This is a statutory requirement for UK organisations.

11.4. Surveillance Cameras

We use surveillance cameras to monitor and record images for the purposes of crime prevention and public safety both inside and outside our buildings. Coverage is designed to minimise any intrusion on reasonable expectations of privacy and we have clear procedures governing the use, retention and disclosure of the personal data we capture which are available in the CCTV policy.

11.5. Generative Artificial Intelligence

This emerging technology:

- stores and learns from the data it is given – this means that any data entered should not identify a living person
- can create believable content, including more credible scam emails requesting payment – research has shown that people interact with generative AI differently than with humans and the content may seem more authoritative and believable.

This school is committed to:

- ensuring we make decisions about using generative AI for the first time ever or using it in completely new ways, by employing the privacy by design approach outlined in section 6 to promote privacy and data protection compliance from the start . We will refer to the DfE Policy paper 'Generative artificial intelligence (AI) in education', the DfE guidance for leaders Using AI in education: support for school and college leaders - GOV.UK, and the DfE resources and support materials in the document 'Using AI in education settings: support materials'. We may also seek a certified assessment of our Safe and effective use of AI in education - Chartered College of Teaching.

- carrying out a DPIA if we feel that new projects or tasks involving generative AI could create a high risk to individuals' interests

- protecting personal and special category data in accordance with data protection legislation

- ensuring all staff receive enough basic information, instruction, training and/or supervision to enable them to work safely with generative AI and without significant risks to their or pupils' health, including mental health e.g., using Cyber Security for Schools - NCSC.GOV.UK and keeping staff updated on emerging risks, recognising and managing them using NSCS blog articles ChatGPT and LLMs: what's the risk and the principles for the security of machine learning

- not allowing or causing intellectual property, including pupils' work, to be used to train generative AI models, without appropriate pupil, student or parental consent or exemption to copyright

- regularly reviewing our cyber risk assessment and strengthening our cyber security to address professional advice we receive, incidents, or changes in risks that we become aware of e.g., generative AI could increase the sophistication and credibility of cyber attacks

- ensuring that children and young people are not accessing or creating harmful or inappropriate content online using generative AI in line with DfE statutory guidance keeping children safe in education in terms of:

- what staff need to do to protect pupils and students online
- how they can limit children's exposure to risks from the school's IT system

For more information about this, see our Online Safety Policy

- ensuring we have appropriate systems in place in line with DfE filtering and monitoring standard to block or restrict harmful content and to help us prevent the misuse of generative AI e.g., to bully others.

All staff have a responsibility to identify when their activities involving generative AI imply the need for a DPIA. This could be doing an entirely new task using generative AI, or it could be changing the way a well-established task is being done to involve AI.

Staff must consult the Deputy Headteacher, and receive agreement to their plans in writing, before using generative AI tools to create original content by pupils or produced from their original work in a new or significantly different way from established practice.

11.6. Transfers of data outside the UK

Transfers of personal data outside the UK are treated differently depending on which countries it is being transferred between or through, what is being transferred, why and how, and how closely those countries' approaches to data protection align with the UK's.

We will follow current IC guidance on International transfers after the UK exit from the EU Implementation Period and Standard Contractual Clauses (SCCs) after the transition period ends for country specific requirements when we need to transfer personal data internationally.

Regarding transfers between the UK and the EU:

When the UK left the EU on 31 January 2020 it entered a "transition" period which kept existing UK-EU data transfer rules aligned as if the UK were still part of the EU ('frozen GDPR'). This allowed freedom of movement for data to continue to flow as before.

On 28 June 2021, the EU approved adequacy decisions for the EU GDPR and the Law Enforcement Directive (LED) i.e. it was agreed that the UK as a third country to the EU ensures an adequate level of protection of the rights and freedoms of EU data subjects to allow transfers. This means that data (excluding data transferred from the EU to the UK for the purposes of UK immigration control) can continue to flow as it did before, in the majority of circumstances until 27 June 2025.

Following the above ICO guidance allows us to continue to meet our data protection obligations. We will also refer new or uncertain international transfers of personal data to or from the UK to our DPO when making decisions about the safety, security, and lawfulness of transferring it.

11.7. Record keeping

The legislation contains some explicit provisions about documenting our processing activities but that is not the reason we keep records. We need to know what data we have and how we use it to be able to control it effectively; we need to be able to justify our decisions about data; and we may need to provide evidence to the ICO as part of a data breach investigation.

We use the ICO GDPR Documentation Template to fully comply with the record keeping required of us under Article 30. It is the responsibility of all staff to ensure the spreadsheet remains a current reflection of how they work with data. Changes to working practices with regard to this should be reported to Darren Best, Senior ICT technician.

We also keep records of our DPIAs, consent, staff training, and our contracts and data sharing agreements i.e. our employment and service provision contracts, processor contracts, and joint-controller data sharing agreements.

We also keep some simple logs which briefly detail:

- SARs;
- other types of data requests and what we did e.g. objection, rectification, withdrawal of consent, education record request etc.;
- data destruction;
- breaches.

All staff are made aware of our record keeping obligations and some staff are specially trained in managing them.

12. Data Sharing

We are required to share personal data with some organisations by law e.g. our census data with the DfE. At other times we share information to improve or protect people's lives and we have included information about this in our Privacy Notices.

All staff are expected to make reference to the current ICO Data Sharing Checklist in making decisions on whether to share data or not and how to do it. Unless the data sharing is routine and pre-authorised e.g. medical data routinely disclosed to the outdoor adventure centres we go on residential trips to, no decision should be made regarding the disclosure of any sensitive personal or sensitive commercial data without reference to an immediate line manager or the headteacher. If nobody involved in the decision-making has received suitable training in data protection, the DPO must be consulted before data is disclosed externally.

With regard to the disclosure of child protection data, we will always follow the current 'Information Sharing Protocol' available from our Local Children's Safeguarding Partnership. Concerns about this type of data sharing must be shared with the Designated Safeguarding Lead (DSL) or deputy DSL before any action is taken to share data.

When we are asked to share personal data with law enforcement agencies, DUAA 2025 only requires us to ensure that the Police etc. have officially provided us with the lawful basis under which we must disclose the data, before we share it. All such requests for personal data must be referred to Steve Bridgman, the DPO, who may then need to consult the DSL/deputy DSL.

We have simple procedures in place regarding unavoidable disclosures to people we do not already have data processing or data sharing agreements with e.g. to an engineer during emergency repair of a computer system, which includes a requirement for them to sign a suitable non-disclosure agreement.

13. Data Retention

We can only keep personal data for as long as we need it. How long that is will depend on the circumstances and the reasons we obtained it.

We will generally follow the guidelines set out in the current Information and Records Management Society 'IRMS Schools Retention guidelines' and we will specifically follow requirements placed on us by our Local Authority and Local Children's Safeguarding Partnership in particular.

We typically retain pupil data and data about their family and other involved professionals until they leave us. Otherwise we retain it for a few days or weeks e.g. trip consent forms, or for 3-50 years depending on whether it is education related or incident related.

We typically retain workforce data for between 6 months and 25 years after an event or the end of their employment with us, depending on their role or if they may have been affected by changes to employment or pension terms ruled by the courts as unlawful. Some pieces of data may need to be retained for 50 years such as records of potential exposure to asbestos, and some indefinitely such as a personnel file when there have been allegations.

We typically retain the personal data of contractors and other professionals in line with work done or contractual agreements, and longer in cases of dispute or allegations.

Some information is retained for more indefinite periods e.g. outreach programme take-up data so that we can analyse trends, or event photographs and accounts so that we can maintain a historical record.

14. Data Disposal

We will dispose of all paper and digital data securely when it is no longer required.

Please see the retention policy for more details on how long data is kept and how it is disposed of.

A Destruction Log will be kept of all data that is disposed of. The log will include any document ID, classification, date of destruction, method and authorisation. The destruction log will be maintained by Senior Technician (Electronic Data) and the Admin Manager (Paper copies of data)

15. Breach Reporting

Any breach of this policy or of data protection laws must be reported to the DPO as soon as practically possible i.e. as soon it becomes apparent. This is so that we can take the right action as soon as possible to put things right and to learn from it so that it cannot happen again. We have a legal obligation to report any qualifying data breaches to the ICO within 72 hours.

A qualifying data breach is one where, if not addressed in an appropriate and timely manner, it could result in physical, material or non-material damage to someone such as loss of control over their personal data or limitation of their rights, discrimination, identity theft or fraud, financial loss, unauthorised reversal of pseudonymisation, damage to reputation, loss of confidentiality of personal data protected by professional secrecy or any other significant economic or social disadvantage to them.

If we experience a data breach and we are unsure whether it is a qualifying data breach that must be reported to the ICO, we will use the ICO self-assessment tool to decide.

All staff and anyone else who owes us or our data subjects a legal duty, a duty of care, or a duty of confidentiality have an obligation to report actual or potential data protection compliance failures. This allows us to:

- investigate the failure and take remedial steps if necessary;
- maintain a register of compliance failures;
- notify the individuals affected; and
- notify the ICO of any compliance failures that are material in their own right or part of a pattern of failures.

Any member of staff who fails to notify of a breach or is found to have known or suspected a breach has occurred but has not followed the correct reporting procedures may be liable to disciplinary action. Where others have been involved in a data breach, a report will also be made to their employer or DPO if relevant to the breach.

16. Our Obligations to our Data Processors

As the data controller we have obligations to our data processors when we give them the personal data of our data subjects which include in general, but are not limited to responsibilities to:

- provide accurate personal data and all necessary corrections in a timely manner;
- employ appropriate technical and organisational security measures when providing and using the personal data being processed;
- only request user access to the data processing for employees and the contractor at a level commensurate with their work tasks and responsibilities e.g. have the fewest possible users who are authorised and enabled to access the accident & incident reporting system which contains sensitive health data;
- respond promptly to requests from our processors for data updates and provide updated and accurate written instruction regarding the continued access to data that we require;

- require our users of any data processor's system to comply with strict password security measures e.g. length, complexity, not shared etc.;
- take appropriate action regarding any breaches;
- ensure our users of a processor's system website understand their responsibilities with regard to the DPA and the GDPR. Anyone found to have carried out unauthorised or unlawful processing activities must be made aware that they will be subject to disciplinary action by you and may be further subject to legal action or prosecution.
- inform our processor as immediately as possible if:
    - we need to remove security access i.e. to our data on their system, from individuals who no longer have any legal right or authority to access it e.g. employees who have left our employment,
    - we need their assistance to comply with a Subject Access Request,
    - we need them to stop processing the personal data of any of our data subjects,
- be sure of our grounds under the law for asking a processor to stop processing the personal data of any of our data subjects and that they are compatible with other applicable laws or legal rights,
- be very sure of our grounds to erase data under the law because we can expect to pay the full costs of any extraordinary measures required to recover erased data where we have failed in our duties.

All staff involved in using the data that we control with the processing services that we contract with have a duty to meet all of our conditions of service. Queries about our contracts for processing activities should be addressed to: Darren Best, Senior ICT technician.

This page is intentionally blank for printing purposes.

Appendix A

Subject Access Request (SAR) Form

Under the Data Protection Act 2018 you have the right to ask us to supply you with a copy of any personal data we hold about you. This form is provided to help you give us the information we need to deal with your request. You do not have to use it but doing so will make it easier for us to respond fully and quickly.

Information supplied in this form will only be used for the purposes of identifying the personal data you are asking for and responding to your request. It will be processed in line with our data protection policy available on the school website.

If you want information about the categories of personal data we collect, our lawful bases for processing it, who we share it with and why, how long we keep it for, and your rights, please see our Privacy Notices available on the school website.

You can complete this form to make a SAR on behalf of someone else (acting as a third party) with their consent.

We aim to respond promptly and within one month of the date we receive your completed SAR form (or request that we recognise as a SAR) *or* the date we receive any further information that we need before we can comply with your request. If we consider your request complex, we can take up to an additional two months to respond. If this is the case, we will let you know within the one-month deadline, and as soon as possible.

We may consider your request complex if it:

- involves retrieval and appraisal of information from multiple sources;
- involves the retrieval of large volumes of information for one data subject which are difficult to separate from information relating to other data subjects;
- is one in a series of requests from the same person;
- involves the release of third-party data for which consent has been refused or cannot be obtained.

For the majority of cases, there is no fee to pay to make this request. However, if the request is deemed excessive or is a manifestly unfounded or repeat request, we may contact you to discuss an appropriate charge.

Before we can process a SAR for:

- Your own personal data, we need to see proof of your identity and address to satisfy us that you are the person legally entitled to have it.
- The personal data of a child you hold parental responsibility for, we need to see proof of your identity and address and proof of your parental responsibility to satisfy us that you are the person legally entitled to have it.
- The personal data of someone else who has asked you to make a request on their behalf as a third-party, we need to see proof of your identity and address, proof of the data subject's identity and address, and proof that the data subject has consented to you making this request for them.

Proof of identity and address in one document can be found on a photocard Driver's Licence.

Other proofs of identity include a current passport (photo page), current national identity card, birth certificate.

Proofs of address must be dated within the last 3 months and could include a bank statement, credit card statement, utility bill, council tax statement, TV licence, HMRC tax document.

Proofs of parental responsibility could include a copy of (please do not include original documents):

Birth mothers (married or unmarried to the birth father) - child's birth certificate naming the child and mother.

Birth fathers (married to the birth mother) - child's birth certificate naming the child and father and the parents' marriage certificate.

Birth fathers (children born after 1 December 2003 when unmarried to the birth mother) - child's birth certificate showing re-registration of the birth after 1 December 2003 and naming the birth father, or a court order e.g. Parental Responsibility Order, or Residence Order, or proof of being appointed the child's Guardian by a Court, by the child's birth mother or by another Guardian, or a Parental Responsibility Agreement with the birth mother.

Birth fathers (children born before 1 December 2003 when unmarried to the birth mother) - child's birth certificate showing re-registration of the birth after 1 December 2003 or any document as for children born before 2003 above.

A person who is not the parent of a child aged 15 or under - a court order like a Residence or Special Guardianship Order, or proof of permission to make the SAR e.g. a signed letter of consent from a person with parental responsibility and/or from the child (if the child is aged 13 or over).

An adoptive parent of a child aged 15 or under - the Adoption Order.

We reserve the right to refuse your request if we are not satisfied you are who you claim to be or if we are unsure whether you have the legal right or valid consent from the data subject to make the request.

For all queries about a SAR, please contact steve.bridgman@st-benedicts.cumbria.sch.uk

Section 1: Subject Access Request Declaration

I am the data subject (the person the information is about): ☐ (Complete Section **2** onwards)
I am acting on behalf of the data subject: ☐ (Complete Section **1a** onwards)

Section 1a: Requestor's Personal Details

Surname: ..... Full Forename(s): .....

My relationship to the data subject is: .....

Children aged 13 or over should make their own SAR unless they do not understand the request.

If you are acting on behalf of a child for whom you have parental responsibility, the child will be asked to consent to the information being released regardless of their age where they have the mental capacity to understand the request:

The child is aged 12 or under so obtaining consent independently of parents or carers may not be appropriate ☐
The child is aged 13-15 and needs to complete a consent slip independently of parents or carers ☐
The young person is aged 16 or 17 and has written and signed a letter of consent (please attach) ☐

If you are acting as a third party on behalf of a data subject:

The data subject has provided consent to disclose the information requested YES ☐ (please attach) NO ☐

Address (if different from the data subject's): .....

.....

Tel. number: ..... Email address: .....

Section 2: Data Subject's Personal Details

Surname: ..... Full Forename(s): .....

Date of Birth: ..... Class or job role: .....

Address: .....

.....

Tel. number: ..... Email address: .....

Section 3: Details of the Subject Access Request

Please provide as much information as possible to help us find the personal data you want e.g. relevant dates or names, or if you believe a particular person or department holds the information, please tell us. *Please note* you are only entitled to personal data about the data subject and not third-party data (information about other people).

Section 4: Proof of Identity, Address, Parental Responsibility, Other Legal Right, and Consent

A person making a SAR must show they have the legal right to do so i.e. that they are the data subject, or they have parental responsibility for the data subject and/or have written consent from them. Data will not be disclosed without proof of identity for the data subject *and* the requestor if different *and* any written consent necessary.
Please list the documents you are providing copies of as proof (see overleaf - please *do not* provide original documents).

Section 5: Data Subject Declaration

I declare that to the best of my knowledge the information I have provided on this form is correct.

Signature of data subject (or parent/carer of): ..... **Date:** .....

Name of data subject (or parent/carer of) **Please print:** .....

Appendix B

School Privacy Notice for Pupils and Parents or Carers

Privacy Notice (How we use pupil information)

St Benedict's Catholic High School is the data controller under the UK General Data Protection Regulation (UK GDPR) for the use of personal data explained in this Privacy Notice.

Personal data is any information that can be used to identify a living person, either on its own, or in combination with other pieces of data. Data processing includes the collection, use, and storage of data.

The categories of pupil and related information that we process include:

- personal identifiers like name, address, unique pupil number, and contact details etc.
- characteristics like ethnicity, language, free school meal, & pupil premium eligibility etc.
- image and voice recordings for assessment, celebration, and in CCTV for safety and security reasons
- safeguarding information like court orders and the involvement of other professionals.
- special educational needs including the needs and ranking.
- medical information like doctors' details, child health, dental health, allergies, medicines, and dietary requirements.
- Financial information like bank details and entitlement to meals, transport, and premium funding to manage catering, school trips etc.
- attendance like sessions attended, absences, absence reasons, previous schools attended.
- assessment and attainment like key stage 2 results, GCSE courses and/or post 16 courses enrolled for and any relevant results.
- behavioural information like behaviour management plans, exclusions, and alternative provision.

Why we collect and use this information

The personal data we collect is essential for the school to fulfil official functions and meet legal requirements and we use it to:

a) support learning,
b) monitor and report on pupil attainment progress,
c) provide appropriate pastoral care,
d) assess the quality of what we do,
e) keep children safe e.g. food allergies, emergency contact details, CCTV,
f) meet the statutory duties placed on us by the Department for Education (DfE), UK Health Security Agency etc.
g) celebrate or promote school, for scientific interest, or to record our own school history.

Under UK GDPR, the lawful bases we rely on for processing personal information about pupils are:

- to perform a public task i.e., to provide education (mainly reasons a, b, c, and d above).
- to protect vital interests (and sometimes carry out a contract too) e.g., to provide **safe** meals, trips, transport, uniform, professional photos, childcare (mainly reasons a, and e above)..
- to comply with the law (mainly reasons b, and f above) e.g., recording attendance, publishing results, recording the census (see Sharing with the DfE below), data sharing with child protection partners like social care, the NHS, and the Local Authority etc. (see sharing with the DfE below for legislation).
- having consent (mainly reason g above, and to process ethnicity data) e.g., use images or names publicly.

When we process special category data like medical information or biometrics, we need to have <u>one</u> lawful basis from the list above *and* <u>one</u> of the following list:

- to prevent medical problems, assess needs, and provide services (mainly reasons e, and f above) e.g., Education Health & Care Plans (EHCP), records of medicines administration.
- to improve public health e.g., report notifiable diseases to local and national government departments;
- to make or defend legal claims e.g., some special educational needs and all accident records.
- having consent (mainly reason h above) e.g., to use biometric data to access catering services.

Collecting pupil data

We collect relevant pupil information via registration forms at the start of each academic year or a secure file sent to us when a child joins us from another school.

Most of the pupil information we ask for is required by law or necessary so we can provide a good education and some of it is voluntary. To comply with UK GDPR, if you have a choice about providing information, we will tell you when we ask for it. We will also tell you what to do if you do not want to share this information with us.

Storing pupil data

We hold pupil data securely in line with the Information and Records Management Society (IRMS) Records Management Toolkit for Schools. This personal data is retained for a wide range of time periods from days after a successful trip for the consent form to many years after a pupil has left us for an accident report. For more information about how long we keep some information for and why (data retention), and how we keep the data safe, please see the data protection policy available from the school.

Who we share pupil information with and why

We do not share information about our pupils with anyone without consent unless the law and our policies allow us to do so. The laws listed in this notice that require us to collect information also require us to share it. Data is transferred securely by hand delivery or registered post, via a government data transfer system like School to School, via a contractor's secure data sharing system like our online school trips safety system, and sometimes in other secure ways.

We routinely share pupil information with:

- Schools and other education providers pupils go to after leaving us to support their continuing education.
- Child development and protection partners like our local Authority Children's Services, Public Health, Inclusion & Social Care etc. to check attendance, monitor, and protect children; the NHS for medical referrals & support; private companies offering counselling and other family or support services.
- The DfE to help decide our school funding, monitor attainment & benchmark it nationally, compile league tables, develop national education policy and monitor it.
- Our Local Authority to ensure they can conduct their statutory duties under the Schools Admission Code, including conducting Fair Access Panels.
- Medical services like therapists, the school nurse, or the NHS for things like screening, vaccinations, health/ eye/ dental checks, Education Health and Care Plan (EHCP) provision etc. and UK Health Security Agency about certain contagious infections our pupils come into contact with.
- Government departments like UK Health Security Agency, Local Authority Public Health, and District Council Environmental Health Departments to comply with the law and support public health action;
- Voluntary and charitable organisations (with your permission only), such as Barnardo's, our local Foodbank and similar organisations who can offer families practical help and support.

Sharing with Youth Support Services

Pupils aged 13 +

Once our pupils reach the age of 13, we pass pupil 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 youth support services and careers advisers

The information shared is limited to the child's name, address, and date of birth. However, where a parent or guardian provides their consent, other information relevant to the provision of youth support services will be shared. This right is transferred to the pupil once they reach the age 16.

Pupils aged 16+

We will also share certain information about pupils aged 16+ with our local authority and / or provider of youth support services because they have responsibilities in relation to the education or training of 13–19-year-olds under the same 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

A pupil once they reach the age of 16 can object to their name, address and date of birth being passed to their local authority or provider of youth support services by informing us.

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

Sharing with the Department for Education (DfE)

The DfE collects personal data from educational settings and local authorities via various statutory data collections (as above). We are required to share this information about our pupils with them directly or via our local authority for the purpose of those data collections, under section 29(3) and section 537A of the Education Act 1996; under the Education (School Performance Information)(England) Regulations 2007; under regulations 5 and 8 of the School Information (England) Regulations 2008; under the Education (Pupil Registration) (England) Regulations 2006; under section 83 of the Children Act 1989 (for monitoring and research purposes); and for census purposes under section 3 of The Education (Information About Individual Pupils) (England) Regulations 2013.

All data is transferred securely and held by DfE under a combination of software and hardware controls, which meet the current government security policy framework.

For more information, please see the section on 'How Government uses your data' below.

Requesting access to your personal data

Under UK GDPR, parents, carers, and pupils 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, please contact Kerry Wilkinson, Admin Manager.

Depending on which lawful basis above was used to process the data, you may also have the right to:

- ask us for access to information about you that we hold
- have your personal data rectified if it is inaccurate or incomplete
- request the deletion or removal of personal data where there is no compelling reason for its continued processing
- restrict our processing of your personal data (i.e., permitting its storage but no further processing)
- object to direct marketing (including profiling) and processing for the purposes of scientific/historical research and statistics
- be subject to decisions based purely on automated processing where it produces a legal or similarly significant effect on you

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

For further information on how to request access to personal information held centrally by DfE, please see the 'How Government uses your data' section of this notice below.

Withdrawal of consent and the right to lodge a complaint

Where we are processing your personal data with your consent, you have the right to withdraw that consent. If you change your mind, or you are unhappy with our use of your personal data, please let us know by contacting steve.bridgman@st-benedicts.cumbria.sch.uk

Last updated

This privacy notice was compiled using DfE advice and model documents. We may need to review it periodically, so we recommend that you revisit this information from time to time. This version was last updated on 29th September 2021.

Contact

If you would like to discuss anything in this privacy notice, please contact: steve.bridgman@st-benedicts.cumbria.sch.uk

How Government uses your data

The pupil data that we lawfully share with the DfE through data collections:

- underpins school funding, which is calculated based upon the numbers of children and their characteristics in each school.
- informs 'short term' education policy monitoring and school accountability and intervention (for example, school GCSE results or Pupil Progress measures).
- supports 'longer term' research and monitoring of educational policy (for example how certain subject choices go on to affect education or earnings beyond school)

Data collection requirements

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

The National Pupil Database (NPD)

Much of the data about pupils in England is held in the National Pupil Database (NPD).

The NPD is owned and managed by the DfE and contains information about pupils 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.

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

Sharing by the DfE

The law allows the DfE to share pupils' personal data with certain third parties, including:

- schools and local authorities
- researchers

- organisations connected with promoting the education or wellbeing of children in England
- other government departments and agencies
- organisations fighting or identifying crime

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

Organisations fighting or identifying crime may use their legal powers to contact DfE to request access to individual level information relevant to detecting that crime. Whilst numbers fluctuate slightly over time, DfE typically supplies data on around 600 pupils per year to the Home Office and roughly 1 per year to the Police.

For information about which organisations the DfE has provided pupil information, (and for which project) or to access a monthly breakdown of data share volumes with Home Office and the Police please visit the following website: https://www.gov.uk/government/publications/dfe-external-data-shares

How to find out what personal information the DfE holds about you

Under the terms of the Data Protection Act 2018, you are entitled to ask the DfE:

- if they are processing your personal data
- for a description of the data they hold about you
- the reasons they're holding it and any recipient it may be disclosed to
- for a copy of your personal data and any details of its source

If you want to see the personal data held about you by the DfE, please make a 'subject access request' to them. Find out how in the DfE's personal information charter published at: www.gov.uk/government/organisations/department-for-education/about/personal-information-charter

To contact the DfE go to: www.gov.uk/contact-dfe.

This page is intentionally blank for printing purposes

Appendix C

School Privacy Notice for Staff

Privacy Notice (How we use school workforce information)

St Benedict's Catholic High School is the data controller under the UK General Data Protection Regulation (UK GDPR) for the use of personal data explained in this notice.

Personal data is any information that can be used to identify a living person, either on its own, or in combination with other pieces of data. Data processing includes the collection, use, and storage of data.

The categories of school workforce information that we process include:

- Personal identifiers like name, address, contact details, employee or teacher number, national insurance number, and image.
- Financial information like bank account, pension, benefits, insurance, and similar details
- Special categories of data like medical information for emergency or occupational health reasons; criminal conviction or social care action information for legal and safeguarding reasons; and protected characteristics information like gender, age, ethnic group etc.
- Contract information like start dates, hours worked, post, roles, salary information, and pre-employment vetting information like references;
- Work absence information like the number of absences and reasons;
- Qualifications and, where relevant, subjects or specialisms taught.

This list is not exhaustive, to see a current list of categories of information we process and why please see the Data Protection Policy available from the school.

Why we collect and use this information

We use school workforce data to:

a) provide us with a comprehensive picture of our workforce, how it is deployed, how it can be developed, and kept safe;

b) recruit appropriately and to inform the development of recruitment and retention policies;

c) enable individuals to be evaluated and developed in their career and be paid

d) meet statutory duties placed on us by HMRC, the Home Office, Department for Education, Department of Work and Pensions, UK Health Security Agency etc.

e) enable individuals to access premises or services we control e.g., .system logins, using biometric recognition;

f) celebrate or promote school, for scientific interest, or to record our own school history.

Under UK GDPR, the lawful bases we rely on for processing personal workforce information are:

- to enter into or carry out a contract (mainly reasons b, c, and e above) e.g., to employ people or buy services for people to use.
- to comply with the law (mainly reasons b, c, and d above) e.g., recording sickness absence for benefits purposes, data sharing with child protection partners like social care, the NHS, and the Local Authority.
- to protect vital interests (mainly reason a above) e.g., allergy or other health information,
- having consent (mainly reasons e, and f above, and to process ethnicity data) e.g., use images and names in publicity (if another basis does not apply), or use biometric data as an identifier.

When we process special category data like medical information, biometrics, or criminal history, we need to have <u>one</u> lawful basis from the list above *and* <u>one</u> of the following list:

- having consent (mainly reasons a, d, and e above) e.g., to use biometric controlled catering services or referral to occupational health or other support services.
- to comply with the law (mainly reason d above) e.g., pre-employment criminal record checks, providing reasonable adjustments for work or interview.
- for preventative or occupational medicine or to assess the work capacity of an employee or to improve public health (mainly reason a above) e.g., report notifiable diseases to local or national government departments;
- to make or defend legal claims (mainly reason d above) e.g., some special educational needs records which include details about the staff involved, and all accident records etc.

Collecting school workforce information

We collect personal information via job application forms and other pre-employment evidence, staff contract forms, staff information sheets.

Most of the information we ask for is required by law or necessary so we can run the school effectively and some of it is voluntary. To comply with UK GDPR, if you have a choice about providing information, we will tell you when we ask for it. We will also tell you what to do if you do not want to share this information with us.

Storing school workforce information

We hold school workforce data securely in line with the Information and Records Management Society (IRMS) Records Management Toolkit for Schools. Most data about staff is kept for between 6 months and 6 years after an event or the ending of a contract, although some is kept for much longer e.g., first aid and accident records that also involved children. Unsuccessful applicant data is kept for 6 months after the date of appointment. For more information about how long we keep some information for and why (data retention), and how we keep the data safe, please see the Data Protection Policy available from the school.

Who we share school workforce information with and why

We do not share information about our workforce with anyone without consent unless the law and our policies allow us to do so. The laws listed in this notice that require us to collect information also require us to share it. Data is transferred securely by hand delivery or registered post, via a government data transfer system like School to School, via a contractor's secure data sharing system like our online school trips safety system, and sometimes in other secure ways.

We share personal data with the Department for Education (DfE) on a statutory basis. This data sharing underpins workforce policy monitoring (see next section).

We also share school workforce information with:

- our payroll and pensions service provider to pay people;
- the Local Government Pension scheme (Your Pension Service) to manage pension contributions;
- HMRC for legal and tax reasons;
- organisations involved with our children like the local authority or other partner professionals who need the names, job titles, contact details and perhaps qualifications of our employees, the places we take children to on trips who might need more personal information like next of kin and medical needs, and workforce development organisations like training providers;
- Government departments like UK Health Security Agency, local authority public health, and District Council Environmental Health Departments to comply with the law and support public health action;
- Occupational Health and similar staff support services only with the consent of the individual.

Department for Education and our Local Authority

The Department for Education (DfE) collects personal data from educational settings and local authorities via various statutory data collections.

The law requires us to share information about our school workforce with the Department for Education (DfE) for the purpose of those data collections, and with our local authority, under section 5 of the Education (Supply of Information about the School Workforce) (England) Regulations 2007 and amendments.

All data is transferred securely and held by DfE under a combination of software and hardware controls which meet the current government security policy framework.

For more information, please see 'How Government uses your data' section.

Requesting access to your personal data

Under UK GDPR, you have the right to request access to information about you that we hold. To make a request for your personal information, contact steve.bridgman@st-benedicts.cumbria.sch.uk

Depending on which lawful basis above was used to process the data, you may also have a right to:

- ask us for access to information about you that we hold
- have your personal data rectified if it is inaccurate or incomplete
- request the deletion or removal of personal data where there is no compelling reason for its continued processing
- restrict our processing of your personal data (i.e., permitting its storage but no further processing)
- object to direct marketing (including profiling) and processing for the purposes of scientific/historical research and statistics
- be subject to decisions based purely on automated processing where it produces a legal or similarly significant effect on you.

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

For further information on how to request access to personal information held centrally by DfE, please see the 'How Government uses your data' section of this notice.

Withdrawal of consent and the right to lodge a complaint

If we are only processing your personal data because you consented, you have the right to withdraw that consent. If you change your mind, or you are unhappy with our use of your personal data, please let us know by contacting steve.bridgman@st-benedicts.cumbria.sch.uk

Last updated

This privacy notice was compiled using DfE advice and model documents. We may need to review it periodically, so we recommend that you revisit this information from time to time. This version was last updated on 29th September 2022.

Contact

If you would like to discuss anything in this privacy notice, please contact:
steve.bridgman@st-benedicts.cumbria.sch.uk

Appendix C

How Government uses your data

The workforce data that we lawfully share with the DfE through data collections:

- informs departmental policy on pay and the monitoring of the effectiveness and diversity of the school workforce
- links to school funding and expenditure
- supports 'longer term' research and monitoring of educational policy

Data collection requirements

To find out more about the data collection requirements placed on us by the Department for Education including the data that we share with them, go to https://www.gov.uk/education/data-collection-and-censuses-for-schools.

Sharing by the Department

The Department may share information about school employees with third parties who promote the education or well-being of children or the effective deployment of school staff in England by:

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

The Department has robust processes in place to ensure that the confidentiality of personal data is maintained and there are stringent controls in place regarding access to it and its use. Decisions on whether DfE releases personal 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 securely store and handle the data

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

How to find out what personal information DfE hold about you

Under the terms of the Data Protection Act 2018, you're entitled to ask the Department:

- if they are processing your personal data
- for a description of the data they hold about you
- the reasons they're holding it and any recipient it may be disclosed to
- for a copy of your personal data and any details of its source

If you want to see the personal data held about you by the DfE, you should make a 'subject access request'. Further information on how to do this can be found in the DfE's personal information charter published at: www.gov.uk/government/organisations/department-for-education/about/personal-information-charter

To contact the department: www.gov.uk/contact-dfe.

School Privacy Notice for Governors

Privacy Notice (How we use governance information)

St. Benedict's Catholic High School is the data controller under the UK General Data Protection Regulation (UK GDPR) for the use of personal data explained in this Privacy Notice.

The categories of governance information that we process include:

- personal information like name, date of birth, gender identity, contact details including address and postcode;
- financial or business information like a governor's outside financial or business interests, or bank details for expense payments;
- Special categories of data like criminal conviction or social care action information for legal and safeguarding reasons, next of kin and medical information (to prevent or manage a health or medical issue), and protected characteristics information like gender identity or religion.
- governance details like their role, start and end dates and governor ID.

Why we collect and use this information

The personal data we collect is essential to fulfil our official functions and meet legal requirements.

We are a maintained school and have a legal duty under section 538 of the Education Act 1996 to provide governance information to the Get Information About Schools (GIAS) scheme online.

We also use governor data to:

a) comply with the law and keep governors safe;
b) recruit appropriately; and
c) enable individuals to be paid expenses.

Under UK GDPR, the lawful bases we rely on for processing personal governance information are:

6(1)(b) to enter into or carry out a contract e.g. to appoint governors, include them in services we buy like access to online subscriptions we hold, or to engage with our training or activity providers.

6(1)(c) to comply with the law e.g. publishing information on our website and submitting data to GIAS.

6(1)(a) having consent e.g. to use images and names in publicity.

When we process sensitive personal information like medical data or criminal history we rely on lawful bases:

9(2)(a) having consent e.g. for referral to occupational health or other support services.

9(2)(b) to comply with the law e.g. pre-appointment criminal record checks, providing reasonable adjustments to governor tasks or election procedures.

9(2)(i) to improve public health e.g. we are required to report infections, like meningitis, Covid-19[1] or e-Coli, to local and national government departments;

9(2)(f) to make or defend a legal claim e.g. all accident records etc.

This list is not exhaustive. For more information about the categories of information we process please see the data protection policy available from the school.

Collecting governance information

[1] Visit: https://www.gov.uk/guidance/maintaining-records-of-staff-customers-and-visitors-to-support-nhs-test-and-trace#information-to-collect, if you want more information about Test and Trace, what data they collect and what they do with it.

We collect personal information via governor application.

Most of the information we ask for is required by law or necessary so we can run the school effectively and some of it is voluntary. To comply with data protection legislation, if you have a choice about providing information, we will tell you when we ask for it.

Storing governance information

We hold governor data securely in line with the Information and Records Management Society (IRMS) Records Management Toolkit for Schools. Most data about governors is kept for between 6 months and 6 years after an election or term of office ends, although some is kept for much longer e.g. minutes of governor meetings showing attendees are kept for the lifetime of a school. For more information about how long we keep some information for and why (data retention), and how we keep the data safe, please the data protection policy available from the school.

Who we share governance information with and why

We do not share information about individuals in governance roles with anyone without consent unless the law and our policies allow us to do so. The laws listed in this notice that require us to collect information also require us to share it. Data is transferred securely by hand delivery or registered post, via a government data transfer system like GIAS, and sometimes in other secure ways.

We routinely share governor information with:

- our local authority (as above),
- our financial services provider to pay expenses;
- Public Health England and, to support test and trace and similar public health emergency action, other partners like the NHS, Local Authority Public Health, and District Council Environmental Health Departments
- other organisations like an off-site training or activity provider that needs next of kin or medical details to manage them safely, and third-party service providers like online subscriptions, but usually only with consent.

Sharing with the Department for Education

The Department for Education (DfE) collects personal data from educational settings and local authorities via various statutory data collections.

We are required to share information about our governors with the Department for Education (DfE) under section 538 of the Education Act 1996.

All data is entered manually on the GIAS system and held by DfE under a combination of software and hardware controls which meet the current government security policy framework.

For more information, please see 'How Government uses your data' section.

Requesting access to your personal data

Under UK GDPR, you have the right to request access to information about you that we hold. To make a request for your personal information, contact steve.bridgman@st-benedicts.cumbria.sch.uk

- Depending on which lawful basis above was used to process the data, you may also have a 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 some circumstances, have inaccurate personal data rectified, blocked, erased, or destroyed; and
- a right to seek redress, either through the ICO, or through the courts

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/.

For more information on how to request access to personal information held centrally by the DfE, please see the 'How Government uses your data' section of this notice.

Withdrawal of consent and the right to lodge a complaint

If we are only processing your personal data because you consented, you have the right to withdraw that consent. If you change your mind, or you are unhappy with our use of your personal data, please let us know by contacting steve.bridgman@st-benedicts.cumbria.sch.uk

Last updated

This privacy notice was compiled using DfE advice and model documents. We may need to review it periodically, so we recommend that you revisit this information from time to time. This version was last updated on 10th September 2021.

Contact

If you would like to discuss anything in this privacy notice, please contact: steve.bridgman@st-benedicts.cumbria.sch.uk

How Government uses your data

The governance data that we lawfully share with the DfE via GIAS will:

- increase the transparency of governance arrangements;
- enable maintained schools and academy trusts and the department to identify more quickly and accurately individuals who are involved in governance and who govern in more than one context;
- allow the DfE to be able to uniquely identify an individual and in a small number of cases conduct checks to confirm their suitability for this important and influential role.

Data collection requirements

To find out more about the requirements placed on us by the DfE including the data that we share with them, go to https://www.gov.uk/government/news/national-database-of-governors

Note: Some of these personal data items are not publicly available and are encrypted within the GIAS system. Access is restricted to a small number of DfE staff who need to see it in order to fulfil their official duties. The information is for internal purposes only and not shared beyond the department, unless the law allows it.

How to find out what personal information DfE hold about you

Under the terms of the UK Data Protection Act 2018, you're entitled to ask the Department:

- if they are processing your personal data;
- for a description of the data they hold about you;
- the reasons they're holding it and any recipient it may be disclosed to;
- for a copy of your personal data and any details of its source.

If you want to see the personal data held about you by the DfE, you should make a 'subject access request'. Further information on how to do this can be found in the DfE's personal information charter published at: www.gov.uk/government/organisations/department-for-education/about/personal-information-charter

To contact the department: www.gov.uk/contact-dfe.

School Privacy Notice for Visitors

Privacy Notice (How we use visitors' information)

St. Benedict's Catholic High School is the data controller under the UK General Data Protection Regulation (UK GDPR) for the use of personal data explained in this Privacy Notice.

Personal data is any information that can be used to identify a living person, either on its own, or in combination with other pieces of data. Data processing includes the collection, use, and storage of data.

The categories of visitor information we process include:

- **Personal data** like your name, employer (if relevant to why you are here), and some location or other data e.g., the date & time you were here, your image on CCTV or an ID badge we give you, your contact number (if we will need to speak to you during or after your visit), your car registration if you are using our car park, and your device address (to allocate you an IP address) if you connect to our wi-fi.
- Special categories of data like a disability we need to accommodate or positive Covid-19 result.

We use this data to comply with the law, for safety and security reasons, deliver education and care, record our work with visitors when we need to (in meeting notes for example)but also to understand who visits us, why, and to improve the visitor experience.

We will keep this information in a visitor management system for 6 years after your visit and it will not be shared with any other organisation. CCTV images are retained for up to 30 days. Personalised badges are destroyed when they are returned on leaving. Depending on the purpose of your visit, information may be retained by us, including in the files of pupils or staff on paper and digitally. We have suitable physical and technical measures in place to protect it.

This does not affect your statutory data protection rights.

If you want to know more or have concerns, please contact [Steve Bridgman, Deputy Headteacher at school, 01946 692275.

Alternatively, you can contact the Information Commissioner's Office at https://ico.org.uk/concerns/.

This page is intentionally blank for printing purposes.

Appendix F

Model Parental Consent Form: Trips, Images and Pain Relief

This form was revised in Sep 2020 only to inform anyone with parental authority that, during a pandemic or other public health emergency, public and private education and childcare facilities do NOT need their or their child's consent to collect personal data and share it with test and trace services. The change to this form has NO effect on any consents you might already hold and this form does NOT need to be re-issued to continuing students. However, adding the paragraph will help you bust widespread myths and reduce unnecessary and time-consuming queries or admin tasks. The style of the form is still a table (ensure 'view grid lines' is on if you want to edit it) but has changed slightly to add class/group and reduce the ink consumed when printed. The intro and some sentences have also been shortened but the substance is the exactly the same.

Educational and other settings which care for children must seek parental consent from those who hold parental responsibility, for several things and this form covers them all to reduce bureaucracy for everyone. **Grey text** is for information only so delete it when done. **Red text** signifies where you need to choose preferred words e.g. school/nursery/college/academy/club etc. or make a special change. If you don't want to ask for all these consents at the same time on one form, delete unwanted sections. Also ensure it is amended to only include what is not asked for elsewhere e.g. on Data Capture Forms i.e. the child's home address and GP Surgery details (name of GP with the full address and telephone number of the Practice) are not asked for here. If you don't request these details elsewhere, add them to this form by inserting rows into the table below.

There is no reference to first aid because failure to give first aid to a child in need is a safeguarding issue so parental consent is not required. Pain relief is not part of first aid therefore consent must be held to administer it. There is no statutory requirement for settings to give pain relief **unless** it would be detrimental to a child's health or school attendance not to do so. This form may also help you identify children and young people who will require a more detailed Individual Health Care Plan in line with your statutory Policy on Supporting Pupils with Medical Conditions.

Dear Parents,

We need parental consent for several things we do at school, so to make life as easy as we can for everyone, we ask for them all at once. The written parental consents below will last for all activities for the duration your child attends this school unless family circumstances which may affect parental responsibility change. **You can withdraw any of these consents at any time.**

We do **not** ask for consent to share your or your child's necessary personal data with any public health authority during a public health emergency like a pandemic. This is because we only need **one** legal reason (lawful basis) to "process" personal data i.e. collect it and give it to someone else. Our lawful reason in any public health emergency, is for the good of public health so that authorities can use the information to protect people. If you want to know more about the rare times when a group or organisation might need consent for this, go to the Information Commissioner's Office website: https://ico.org.uk/global/data-protection-and-coronavirus-information-hub/coronavirus-recovery-data-protection-advice-for-organisations/collecting-customer-and-visitor-details-for-contact-tracing/.

Educational Visits

Please read the declarations, complete the medical information section, and tell us who your two main emergency contacts are should your child experience an emergency at school or off-site.

The Use of Your Child's Name, Image and Voice

We don't need parental consent to use personal data, including image or voice recordings when we use it for education purposes. Using the names, images, and voices of children in their work and in displays inside school is a fundamental part of their education, personal development and how we celebrate them. This does not affect your or your child's statutory rights (described in our Privacy Notice). Anyone can raise any concern with any member of staff about our use of their or their child's data at any time and we must ensure the rights of the individual are upheld if we have no good reason to refuse.

We do need parental consent to use personal data for other reasons like marketing or self-promotion in print and on websites or social media directly managed by us or, with our permission, by others associated with us and this may include pictures that have been drawn by children. Images that might cause embarrassment or distress will not be used, nor will your child's image or voice be associated with materials or issues that are considered sensitive. You can ask to see any images that we hold of your child at any time.

Photography, audio recording or filming will only take place during school activities with the permission of the Head teacher, and under appropriate supervision.

Regardless of who is doing the publishing, our policy is that children will only be named if there is a good reason e.g. they have won a prize, and no other personal details will be published or given out. If names will, or might be published e.g. in a newspaper article, we will check that you consent at the time and before the publishing happens. It is important to understand that if you do consent, the images and your child's name will appear in local or national newspapers and worldwide online.

If you want to attend school functions and record your child, please be sensitive to other people and try not to disrupt concerts, performances and events. Please also bear in mind that you may capture other people's children so make sure images are appropriate. If you or your child intends to share images, you can only share them publicly i.e. post them to social media, with the express permission of the parents of everyone in the images. Please also note that we ask all parents, carers, and children to support our approach to online safety and to not upload or post to the internet any pictures, audio, video, or text that could upset, offend, or threaten the safety of any member of the school community or bring the school into disrepute. If these rules are not respected, governors reserve the right to stop everyone from recording school events.

Please carefully consider the consent descriptions in the form below and tell us what you consent to by crossing out "do" or "do not" as applicable.

Giving Medicines (necessary pain relief only)

We will not give your child any medicine, including pain relief, unless it is in line with our policy for Supporting Pupils with Medical Conditions (available on request) **and** you give your express consent

If your child requires regular medicine for a health or medical condition, we will need more detailed information about it and as part of your child's Individual Healthcare Plan you will be asked for that separately.

Appendix F

Parental Consent Form - Trips, Images and Pain Relief

Name of Child: ..... **Date of Birth:** ..... **Class/ Group:** .....

EDUCATIONAL VISITS

This consent will last for the entire time your child is with us at this school, but it is good practice for us to check your consent still applies when we offer residential or adventurous visits. When we tell you about them, we will ask for current information about your child e.g. updated medical needs, sleepwalking, swimming ability etc. and offer you the chance to withdraw your consent. You should also complete and return any slip provided then.

Declaration *Please delete as applicable

I ***do / do not** consent to my child taking part in school trips and other activities that take place off-site **and** to them being given urgent medical or dental treatment or necessary pain relief during any trip or activity.

I understand that:

- **All** trips and activities are covered by this consent and will include;
  - all visits (including residential trips) which take place during the holidays or a weekend,
  - adventure activities at any time *and*
  - off-site sporting fixtures outside the normal school day,
- School will provide me with information about each trip or activity before it takes place.
- I can inform school that I **do not** want my child to take part in a particular trip/activity and I should do so in writing.
- I **must** ensure that I and my child understand and agree to abide by any trip Code-of-Conduct.
- I **must** keep school informed if any medical information I have provided becomes out-of-date or where religious beliefs may impact on any medical treatment my child may receive.
- I **must** keep school informed if any emergency contact information I have provided becomes out-of-date or does not apply to a particular trip and I must provide alternatives as necessary.
- All school activities are appropriately insured. I also understand the extent and limitations of this insurance (details available on request).

Medical Information: Details of any medical conditions including allergies and travel sickness that my child suffers from and any medicines with dosage etc. that they should take during off-site activities including those outside school hours or overnight – attach additional sheet if necessary.

Using ParentPay and Edulink to stay in touch:

To keep up to date with information about school, particularly activities, visits and fixtures:

I ***can / cannot** use the school apps ParentPay and Edulink

EMERGENCIES:	**Emergency Contact 1**		**Emergency Contact 2**	
Name:				
Relationship:				
Telephone Number(s):	Work:		Work:	
	Home:		Home:	
	Mobile:		Mobile:	

Appendix F

USE OF YOUR CHILD'S IMAGE AND VOICE *please delete as applicable

I ***do / do not*** consent to photos, video, or audio recordings of my child being published in media *which school directly controls*, including online available worldwide e.g. the prospectus, the school website, school Twitter feed, school Facebook page.

I ***do / do not*** consent to photos, video, or audio recordings of my child being published in media *which school does **not** directly control*, including online available worldwide i.e. outside organisations which school has carefully selected e.g. news media, other websites publicising events that your child participated in etc.

Declaration

I understand that any photos, video, or audio recordings I might make at school events must not be used inappropriately **and** that they cannot be shared publicly without suitable consent from everyone in them. I also understand that if these rules are not respected, governors reserve the right to stop everyone from recording school events.

NECESSARY PAIN RELIEF (Paracetamol)

I understand that my child will not be given any medicine, including necessary pain relief, unless it would be detrimental to their health or school attendance not to **and** express consent is given here. *Please delete as applicable.

I ***do / do not*** consent to my child receiving necessary pain relief medicine (Paracetamol) in line with the school policy and as per my instructions or those of a medical practitioner. I understand that if my child will require the regular administration of medicine at school, even for a limited time, I **must** complete a different form giving more detail.

By signing this form, I confirm I have read the information above, I understand the declarations and I have deleted as applicable to clearly show what parental consent is given and what is not given.

Signed: ..... Relationship to Child: .....

Print Name: ..... Date: .....

Data Classifications and Handling Requirements

This is an indicative rather than exhaustive guide to data classification and the resulting data handling requirements. All relevant queries should be directed to the Data Protection Officer or the Data Protection Support Assistant or the Information Technology Manager.

	Public	Confidential	Sensitive
Impact if the information becomes public	**No risk**	**Low-Medium Risk** May result in minor reputational or financial damage to the school. May result in minor privacy breach for an individual.	**Medium-High Risk** Could substantially damage the reputation of the school, have a substantial financial effect on school or a third party, or would result in a serious privacy breach to one or more individuals.
Description of the information	Information that does not require protection and is considered "open and unclassified" and which may be seen by anyone whether directly linked with school or not. Information is likely to already exist in the public domain.	May result in minor reputational or financial damage to the school. May result in a minor privacy breach for an individual. Information that should only be available to sub-groups of staff within the school who need the information to carry out their roles.	Information that has the potential to cause serious damage or distress to individuals or serious damage to the school's interests if disclosed inappropriately. Information which is sensitive in some way because it might be sensitive personal data, commercially sensitive, legally privileged or under embargo. This information should only be available to a small tightly restricted group of authorised users.
Examples of information This list is indicative not exhaustive if unsure ask Steve Bridgman for advice	● Prospectus ● Press releases ● Open content on the school web site ● Publicity flyers and leaflets ● Published information released under the Freedom of Information Act ● Policies, annual reports and financial statements ● Job adverts (excluding internal only positions) ● staff names and contact details ● Staff publications. ● Agendas and minutes of school committees and working groups (except reserved business). ● Patented intellectual property.	● Student personal details e.g. demographics, personal email address etc. ● Staff personal details e.g. demographic, payroll number, personal email address etc. ● Internal only school policies, processes and guidelines. ● Internal only job adverts. ● Tender bids prior to award of contract ● Individual's salaries ● Student's assessment marks. ● Job application responses/CVs (unless they contain sensitive personal information).	Sensitive personal data and some other data. ● Exam questions prior to use ● Medical records ● UPRNs ● Usernames and passwords ● Investigations/disciplinary proceedings. ● Payment card details. ● Financial information (banking details and data not already disclosed in financial statements). ● Passwords and access codes to school systems. ● Some complaints or requests ● Biometric data
Security Marking	No marking required	Must be clearly marked as **Confidential**	Must be clearly marked as **Sensitive**

	Public	Confidential	Sensitive
Storage (electronic)	● Store using school IT facilities to ensure appropriate management, back-up and access. ● Use only the school approved cloud services. Some cloud services may **not** be used because they link to computer C: drives which is not secure. If you are unsure of the approved cloud services ask Darren Best, Senior IT Technician	● Store only on the school IT network and never on the C: drive of a PC/laptop (beware downloading information when a laptop is not connected to the school domain - the download will go onto the C: drive and you may be in breach of this policy). ● Store only on the C: drive of a specially encrypted PC/laptop. ● Store only on the approved cloud service in a suitably restricted folder. ● Portable devices such as USB sticks must be encrypted and must **not** be used for long term storage due to the risks of loss or corruption of data. ● Never to be stored on any personal device or personal cloud service not controlled by school or on any unencrypted school device e.g. tablet, laptop, mobile phone etc.	● Store only on the school IT network in rigorously monitored & restricted access drives. ● Never to be stored on the approved cloud service unless also separately encrypted. ● Never to be stored on any portable storage device i.e. USB drive regardless of encryption. ● Never to be stored on any personal device or personal cloud service not controlled by school or on any school device e.g. tablet, laptop, mobile phone etc. unless it has been specially encrypted *and* there are other high level procedural safeguards.
School Website	No restrictions	Not permitted	Not permitted
Storage (hardcopy)	No restrictions	In a lockable cabinet/drawer which is locked when unattended and where the room is also locked when unoccupied. If not in a lockable store the room where this classification of data is kept should be locked at all times when unattended and must have restricted access.	In a lockable cabinet/drawer which is locked when unattended and where the room is also locked when unoccupied. If not in a lockable store the room where this classification of data is kept should be locked at all times when unattended and must have restricted access.
Email hosted by school	No restrictions	Emails to external recipients must not contain this data. It must be an encrypted email or sent as an encrypted attachment and the password conveyed by a separate mechanism e.g. telephone. Emails to internal recipients i.e. school email account-to-school email account are secure, so encryption and encrypted attachments are not necessary.	Emails to external recipients must not contain this data. It must be an encrypted email or sent as an encrypted attachment and the password conveyed by a separate mechanism e.g. telephone. Emails to internal recipients i.e. school email account-to-school email account are secure, so encryption and encrypted attachments are not necessary.
Personal email account e.g. Hotmail etc.	No restrictions	Not permitted	Not permitted
Post (Internal)	No restrictions	In a sealed envelope marked Confidential.	Seal envelope, mark Confidential & hand deliver.

	Public	Confidential	Sensitive
Post (External)	No restrictions	Tracked and recorded delivery only and marked Confidential	Tracked and recorded delivery only and marked Confidential within two separate envelopes.
School-based server	No restrictions but consideration should be given to back-up requirements.	No storage or creation is permitted unless the server environment is equivalent to the school-based server or the CTU server environment.	No storage or creation permitted unless the server environment is equivalent to the school-based server or the CTU server environment.
School owned laptop	No restrictions but do **not** use to store master copies of vital records.	The internal storage (hard drive(s), HDDs, SSDs) must be encrypted and set to lock after five minutes of inactivity.	The internal storage (hard drive(s), HDDs, SSDs) must be encrypted and set to lock after five minutes of inactivity.
Personally owned mobile device	No restrictions	Only to be stored on devices that are encrypted and have PIN/password/Biometric access controls applied in line with the ICO BYOD guidance document.	Not permitted unless authorised by the Senior Information Risk Owner (SIRO). Only then to be stored on devices that are encrypted and have PIN/password/Biometric access controls applied in line with the ICO BYOD guidance document.
School owned desktop (public areas)	No restrictions, but always lock the screen when unattended.	Not permitted. The risk of incidental disclosure is too high.	Not permitted. The risk of incidental disclosure is too high.
School owned desktop (key/card access controlled areas)	No restrictions, but always lock the screen when unattended.	Only permitted on encrypted drives or using or password protected files. Always lock the screen when unattended.	Only permitted on encrypted drives. Always lock the screen when unattended.
School owned mobile device	No restrictions, but always lock the screen when unattended.	Only to be stored on devices that are encrypted and have PIN/password/Biometric access controls applied in line with our policy and the ICO BYOD guidance document.	Not permitted unless authorised by the SIRO. Only then to be stored on devices that are encrypted and have PIN/password/Biometric access controls applied in line with our policy and the ICO BYOD guidance document
Removable media (CDs, USB drives etc.)	No restrictions.	Encrypted storage with strong password e.g. 8 characters or longer and a mixture of uppercase, lowercase, digits and special characters.	Encrypted storage with strong password e.g. 8 characters or longer and a mixture of uppercase, lowercase, digits and special characters.
Disposal	No restrictions. Recycle where possible.	Shred or place in a confidential waste bag. Delete from electronic media when no longer required.	Cross shred only & put shredded material into the confidential waste. Appropriately scrub data from devices. Some devices (encrypted USB drives) may need to be securely destroyed. Seek advice from the IT manager.