Policy: Data Protection (UK GDPR Compliant)

Date: April 2025

Relevant supportive documents and legislation:

- Freedom of information publication scheme
- Computing and Internet Safety Policy
- Remote Learning Policy
- Data Compliance Plan (DCP)
- Parental Permission, Consent and Agreements
- Staff Consent Forms
- ICT Acceptable Use Policy
- Code of Practice
- Child Protection and Safeguarding Policy
- UK GDPR & Data Protection Act 2018
- In the picture: A data protection code of practice for surveillance cameras and personal information (ICO)
- School Privacy Statements – staff and parents

Date created: March 2018, amended March 2019, updates March 2020, amendments March 2021 and March 2022, April 2023, April 2024 and April 2025

Responsible: Headteacher

Date Ratified: 16th April 2018

Responsible Committee: FGB under the recommendations of the GDPR Lead Governor and DPO

Date to be reviewed: Annually in March unless otherwise required due to new legislation

Statutory Policy: Y

This Policy is based on a policy written in partnership with **Emma Swann**, education consultant and approved by Forbes Solicitors.

Contents

1. Aims

Our school aims to ensure that all personal data collected about staff, pupils, parents, governors, visitors and other individuals is collected, stored and processed in accordance with UK data protection law.

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

2. Legislation and guidance

This policy meets the requirements of the:

- UK General Data Protection Regulation (UK GDPR) – the EU GDPR was incorporated into UK legislation, with some amendments, by The Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2020
- Data Protection Act 2018 (DPA 2018)

It is based on guidance published by the Information Commissioner's Office (ICO) on the UK GDPR and guidance from the Department for Education (DfE) on Generative artificial intelligence in education.

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

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

3. Definitions

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

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

4. The data controller

Our school processes personal data relating to parents, pupils, staff, governors, visitors and others, and therefore is a data controller.
The school is registered with the ICO and has paid its data protection fee to the ICO, as legally required.

5. Roles and responsibilities

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

5.1 Governing board

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

5.2 Data protection officer

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

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

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

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

Please find below details of the School's Data Protection Officer: -

Data Protection Officer: Judicium Consulting Limited

Address: 5th Floor, 98 Theobalds Road, London, WC1X 8WB

Email: dataservices@judicium.com

Web: www.judiciumeducation.co.uk

Telephone: 0345 548 7000 option 1 then option 1 again

5.3 Headteacher

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

5.4 All staff

Staff are responsible for:

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

6. Data protection principles

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

The principles say that personal data must be:

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

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

7. Collecting personal data

7.1 Lawfulness, fairness and transparency

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

- The data needs to be processed so that the school can **fulfil a contract** with the individual, or the individual has asked the school to take specific steps before entering into a contract
- The data needs to be processed so that the school can **comply with a legal obligation**
- The data needs to be processed to ensure the **vital interests** of the individual e.g. to protect someone’s life

- The data needs to be processed so that the school, as a public authority, can perform a task **in the public interest or exercise its official authority**

- The data needs to be processed for the **legitimate interests** of the school (where the processing is not for any tasks the school performs as a public authority) or a third party, provided the individual's rights and freedoms are not overridden
- The individual (or their parent/carer when appropriate in the case of a pupil) has freely given clear **consent**

For special categories of personal data, we will also meet one of the special category conditions for processing under data protection law:

- The individual (or their parent/carer when appropriate in the case of a pupil) has given **explicit consent**
- The data needs to be processed to perform or exercise obligations or rights in relation to **employment, social security or social protection law**
- The data needs to be processed to ensure the **vital interests** of the individual or another person, where the individual is physically or legally incapable of giving consent
- The data has already been made **manifestly public** by the individual
- The data needs to be processed for the establishment, exercise or defence of **legal claims**
- The data needs to be processed for reasons of **substantial public interest** as defined in legislation
- The data needs to be processed for **health or social care purposes**, and the processing is done by, or under the direction of, a health or social work professional or by any other person obliged to confidentiality under law
- The data needs to be processed for **public health reasons**, and the processing is done by, or under the direction of, a health professional or by any other person obliged to confidentiality under law
- The data needs to be processed for **archiving purposes**, scientific or historical research purposes, or statistical purposes, and the processing is in the public interest

For criminal offence data, we will meet both a lawful basis and a condition set out under data protection law. Conditions include:

- The individual (or their parent/carer when appropriate in the case of a pupil) has given **consent**
- The data needs to be processed to ensure the **vital interests** of the individual or another person, where the individual is physically or legally incapable of giving consent
- The data has already been made **manifestly public** by the individual
- The data needs to be processed for or in connection with legal proceedings, to obtain legal advice, or for the establishment, exercise or defence of **legal rights**
- The data needs to be processed for reasons of **substantial public interest** as defined in legislation

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

We will always consider the fairness of our data processing. We will ensure we do not handle personal data in ways that individuals would not reasonably expect, or use personal data in ways which have unjustified adverse effects on them.

7.2 Limitation, minimisation and accuracy

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

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

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

We will keep data accurate and, where necessary, up-to-date. Inaccurate data will be rectified or erased when appropriate.

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

8. Sharing personal data

We will not normally share personal data with anyone else without consent, but there are certain circumstances where we may be required to do so. These include, but are not limited to, situations where:

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

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

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

Where we transfer personal data internationally, we will do so in accordance with UK data protection law.

9. Subject access requests and other rights of individuals

9.1 Subject access requests

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

- Confirmation that their personal data is being processed
- Access to a copy of the data
- The purposes of the data processing
- The categories of personal data concerned
- Who the data has been, or will be, shared with
- How long the data will be stored for, or if this isn't possible, the criteria used to determine this period
- Where relevant, the existence of the right to request rectification, erasure or restriction, or to object to such processing
- The right to lodge a complaint with the ICO or another supervisory authority
- The source of the data, if not the individual
- Whether any automated decision-making is being applied to their data, and what the significance and consequences of this might be for the individual
- The safeguards provided if the data is being transferred internationally

Subject access requests can be submitted in any form, but we may be able to respond to requests more quickly if they are made in writing and include:

- Name of individual
- Correspondence address

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

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

9.2 Children and subject access requests

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

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

9.3 Responding to subject access requests

When responding to requests, we:

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

We may not disclose information for a variety of reasons, such as if it:

- Might cause serious harm to the physical or mental health of the pupil or another individual
- Would reveal that the child is being or has been abused, or is at risk of abuse, where the disclosure of that information would not be in the child's best interests
- Would include another person's personal data that we can't reasonably anonymise, and we don't have the other person's consent and it would be unreasonable to proceed without it
- Is part of certain sensitive documents, such as those related to crime, immigration, legal proceedings or legal professional privilege, management forecasts, negotiations, confidential references, or exam scripts

If the request is unfounded or excessive, we may refuse to act on it, or charge a reasonable fee to cover administrative costs. We will take into account whether the request is repetitive in nature when making this decision.

When we refuse a request, we will tell the individual why, and tell them they have the right to complain to the ICO or they can seek to enforce their subject access right through the courts.

9.4 Other data protection rights of the individual

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

- Withdraw their consent to processing at any time
- Ask us to rectify, erase or restrict processing of their personal data (in certain circumstances)
- Prevent use of their personal data for direct marketing
- Object to processing which has been justified on the basis of public interest, official authority or legitimate interests
- Challenge decisions based solely on automated decision making or profiling (i.e. making decisions or evaluating certain things about an individual based on their personal data with no human involvement)
- Be notified of a data breach in certain circumstances

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

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

10. Parental requests to see the educational record

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

If the request is for a copy of the educational record, the school may charge a fee to cover the cost of supplying it.

This right applies as long as the pupil concerned is aged under 18.

There are certain circumstances in which this right can be denied, such as if releasing the information might cause serious harm to the physical or mental health of the pupil or another individual, or if it would mean releasing exam marks before they are officially announced.

11. CCTV

We use CCTV in various locations around the external area of the school site and inside the entrance doors of the main reception area to ensure the site remains safe. We will follow the ICO's guidance for the use of CCTV, and comply with data protection principles.

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

Any enquiries about the CCTV system should be directed to the school Site Manager.

Further details can be found within our school's CCTV Policy

12. Photographs and videos

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

We will obtain written consent from parents/carers for photographs and videos to be taken of their child for communication, marketing and promotional materials. We will clearly explain how the photograph and/or video will be used to both the parent/carer and pupil. See Appendix 2 for Consent Forms

Any photographs and videos taken by parents/carers at school events for their own personal use are not covered by data protection legislation. However, we will ask that photos or videos with other pupils are not shared publicly on social media for safeguarding reasons, unless all the relevant parents/carers have agreed to this.

Uses may include:

- Within school on notice boards and in school magazines, brochures, Foundation Stage *Ey-log* electronic learning journeys, *Google Classroom*, newsletters, etc.
- Outside of school by external agencies such as the school photographer, newspapers, campaigns, websites promoting the activities of our school
- Online on our school website or social media pages

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

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

See our Computing and Internet Safety Policy for more information on our use of photographs and videos.

13. Artificial intelligence (AI)

Artificial intelligence (AI) tools are now widespread and easy to access. Staff, pupils and parents/carers may be familiar with generative chatbots such as ChatGPT, Copilot and Google Bard. St Bernadette's recognises that AI has many uses to help pupils learn, but also poses risks to sensitive and personal data.

To ensure that personal and sensitive data remains secure, no-one will be permitted to enter sensitive or personal data, or any information that allows a child or colleague to be identified into generative AI tools or chatbots.

If personal and/or sensitive data is entered into a generative AI tool, St Bernadette's will treat this as a data breach, and will follow the personal data breach procedure outlined in appendix 1.

14. Data protection by design and default

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

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

15. Data security and storage of records

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

In particular:

- Paper-based records and encrypted portable electronic devices, such as laptops and hard drives that contain personal data are kept under lock and key when not in use
- Papers containing confidential personal data must not be left on office and classroom desks, on staffroom tables, or left anywhere else where there is general access
- Where personal information needs to be taken off site, staff must sign it in and out from the school office
- Passwords that are at least 10 characters long containing letters and numbers are used to access school computers, laptops and other electronic devices. Staff and pupils are reminded that they should not reuse passwords from other sites

- Encryption software is used to protect *all* devices and removable media, for example, laptops and USB devices
- Staff, pupils or governors must not store personal information on their personal devices and are expected to follow the same security procedures as for school-owned equipment (see our Computer and Internet safety policy and acceptable use agreement)
- Where we need to share personal data with a third party, we carry out due diligence and take reasonable steps to ensure it is stored securely and adequately protected (see section 8)
- Printing is protected by a secure release system. Documents printed internally containing sensitive information can only be released at the machine with the exact fob or PIN owned by the sender.

16. Disposal of records

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

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

17. Personal data breaches

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

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

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

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

18. Training

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

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

19. Monitoring arrangements

The Full Governing Board, under the advice of the DPO and GDPR Lead Governor is responsible for monitoring and reviewing this policy.

This policy will be reviewed annually in April.

Appendix 1: Personal data breach procedure

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

On finding or causing a breach, or potential breach, the staff member, governor or data processor must immediately notify the Data Protection Officer

Please find below details of the School's Data Protection Officer: -

Data Protection Officer: Judicium Consulting Limited

Address: 5th Floor, 98 Theobalds Road, London, WC1X 8WB

Email: dataservices@judicium.com

Web: www.judiciumeducation.co.uk

Telephone: 0345 548 7000 option 1 then option 1 again

- The DPO will investigate the report, and determine whether a breach has occurred. To decide, the DPO will consider whether personal data has been accidentally or unlawfully:
    - Lost
    - Stolen
    - Destroyed
    - Altered
    - Disclosed or made available where it should not have been
    - Made available to unauthorised people
- Staff and governors will cooperate with the investigation (including allowing access to information and responding to questions). The investigation will not be treated as a disciplinary investigation
- If a breach has occurred or it is considered to be likely that is the case, the DPO will alert the headteacher and the chair of governors
- The DPO will make all reasonable efforts to contain and minimise the impact of the breach. Relevant staff members or data processors should help the DPO with this where necessary, and the DPO should take external advice when required (e.g. from IT providers). (See the actions relevant to specific data types at the end of this procedure)
- The DPO will assess the potential consequences (based on how serious they are and how likely they are to happen) before and after the implementation of steps to mitigate the consequences
- The DPO will work out whether the breach must be reported to the ICO and the individuals affected using the ICO's self-assessment tool
- The DPO will document the decisions (either way), in case the decisions are challenged at a later date by the ICO or an individual affected by the breach. Documented decisions are stored on the school's O-drive GDPR file.
- Where the ICO must be notified, the DPO will do this via the 'report a breach' page of the ICO website, or through its breach report line (0303 123 1113), within 72 hours of the school's awareness of the breach. As required, the DPO will set out:
    - A description of the nature of the personal data breach including, where possible:
        - The categories and approximate number of individuals concerned
        - The categories and approximate number of personal data records concerned
    - The name and contact details of the DPO
    - A description of the likely consequences of the personal data breach
    - A description of the measures that have been, or will be taken, to deal with the breach and mitigate any possible adverse effects on the individual(s) concerned

- If all the above details are not yet known, the DPO will report as much as they can within 72 hours. The report will explain that there is a delay, the reasons why, and when the DPO expects to have further information. The DPO will submit the remaining information as soon as possible
- Where the school is required to communicate with individuals whose personal data has been breached, the DPO will tell them in writing. This notification will set out:
  - A description, in clear and plain language, of the nature of the personal data breach
  - The name and contact details of the DPO
  - A description of the likely consequences of the personal data breach
  - A description of the measures that have been, or will be, taken to deal with the data breach and mitigate any possible adverse effects on the individual(s) concerned

The DPO will consider, in light of the investigation and any engagement with affected individuals, whether to notify any relevant third parties who can help mitigate the loss to individuals – for example, the police, insurers, banks or credit card companies

› The DPO will document each breach, irrespective of whether it is reported to the ICO. For each breach, this record will include the:

- Facts and cause
- Effects
- Action taken to contain it and ensure it does not happen again (such as establishing more robust processes or providing further training for individuals)

Records of all breaches will be stored within a confidential drive on the school's computer system which has restricted access.

The DPO and headteacher will meet to review what happened and how it can be stopped from happening again. This meeting will happen as soon as reasonably possible

Actions to minimise the impact of data breaches

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

Sensitive information being disclosed via email (including safeguarding records)

- If special category data (sensitive information) is accidentally made available via email to unauthorised individuals, the sender must attempt to recall the email as soon as they become aware of the error
- Members of staff who receive personal data sent in error must alert the sender and the DPO as soon as they become aware of the error
- If the sender is unavailable or cannot recall the email for any reason, the DPO will ask the ICT department to recall it from external recipients and remove it from the school's email system (retaining a copy if required as evidence)
- In any cases where the recall is unsuccessful, the DPO will consider whether it's appropriate to contact the relevant unauthorised individuals who received the email, explain that the information was sent in error, and request that those individuals delete the information and do not share, publish, save or replicate it in any way
- The DPO will endeavor to obtain a written response from all the individuals who received the data, confirming that they have complied with this request
- The DPO will carry out an internet search to check that the information has not been made public; if it has, we will contact the publisher/website owner or administrator to request that the information is removed from their website and deleted
- If safeguarding information is compromised, the DPO will inform the designated safeguarding lead and discuss whether the school should inform any, or all, of its 3 local safeguarding partners

- The member(s) of staff who disclosed the information will then be appropriately addressed in line with procedures and disciplines outlined in the *Data Protection Staff Agreement.*

Details of pupil premium interventions for named children being published on the school website.

- The first action should be to immediately approach the website administrators (in this instance 'Primary Site') and request the content is immediately taken down. If this isn't possible in a timely manner; action should be taken (by a member of staff with appropriate permissions) to login to the website and take down the content.
- The incident should then be raised with the DPO who may relay findings, depending on the severity of the breach, to the ICO. This will detail the time, date, location and duration of which the document was visible publicly.
- Further to this: the DPO will consider the impact and severity of the data breached by working alongside the headteacher, whom will have knowledge of the offending document, and provide advice relating to the impact of those involved. Parents, staff and any other relevant individuals will then be informed of the breach, and the school's assessment of the potential impact to the unintentional release of their data.
- The school in conjunction with the DPO officer will offer advice to these individuals on what to do next, including information on how to seek advice and report the incident to the ICO. The DPO will then compile and submit a report to the school governors detailing the breach.
- The member(s) of staff who uploaded the document will then be appropriately addressed in line with procedures and disciplines outlined in Data Protection Staff Agreement.

Non-anonymised pupil exam results or staff pay information being shared with governors

- All school-related information is shared with governors via school email addresses. Any governor who receives non-anonymised data of this nature must alert the sender and the DPO. The DPO will contact all governors, explain that the information was sent in error and request that they delete the information and do not share, publish, save or replicate it in any way
- The DPO will ensure we receive a written response from all the individuals who received the data, confirming that they have complied with this request
- The DPO will ensure that any hard copies held by governors are shredded on school property and that this is witnessed and evidence signed and kept as evidence of the destruction of the copies.
- The member(s) of staff who shared the information will then be appropriately addressed in line with procedures and disciplines outlined in the *Data Protection Staff Agreement.*

In the event that a school laptop containing non-encrypted sensitive personal data is stolen or hacked.

- *The laptop owner upon discovering the breach must immediately notify the Headteacher and DPO in the first instance, then IT Support immediately afterwards. The laptop owner will have their access temporarily revoked; during which time all passwords relating to the laptop owner will be changed (including VPN access) and support will be given to the member of staff regarding changing personal passwords on other owned accounts.*
- *Where theft is suspected, the event will also be reported to the police as soon as possible and a statement taken from the member of staff with regards to whereabouts and situation.*
- *The assessment of severity and impact of the breach will then be arrived at with the member of staff and action taken appropriately. The DPO will then compile a report and submit to the school, they may report this breach to the ICO should the impact assessment justify this outcome.*
- The member(s) of staff who uploaded the document will then be appropriately addressed in line with procedures and disciplines outlined in the *Data Protection Staff Agreement.*

Appendix 2

Parental Permission, Consent and Agreements

Dear Parents and Carers,

The following paragraphs outline activities for which we need to obtain your specific permission, consent or agreement (PCAs). Your PCAs will stand for the time your child is at St Bernadette's or until legislation requires us to amend the details.

Parents and carers may withdraw PCAs at any time; this must be done formally in a letter addressed to the Headteacher. The Headteacher will respond in writing within two weeks of receipt of withdrawal of PCAs.

Please read each statement carefully and respond with either Yes or No to demonstrate whether you are or are not providing your permission, consent or agreement.

Our Privacy Notices can be found on our website: https://www.stbernadettesschool.com/school-policies/

Yours faithfully

Mrs Zamora (Headteacher)

CHILD'S NAME …… Date of birth ……/……./……

THE LIBRARY

Our library books are barcoded and information about each book is held on the computer. We ask you to ensure that all books taken home are treated with care and returned promptly. You will appreciate that books are expensive and if they are lost you will be responsible for the cost of any necessary replacement.

I give my permission for my child to borrow books from the library and agree to ensure that any borrowed library book is returned on time. I understand that I am responsible for the cost of replacing any lost or damaged book

Yes □ No □

PHOTOGRAPHS/IMAGES/PUPILS' WORK

We like to take photographs of our pupils which may be used for displays, as records of work/events, for publication in the diocesan/local press or on the school website, prospectus or other printed publications that the school may produce for informative or promotional purposes. **Names of children will not be published alongside photographs**. As part of the Computing curriculum, we may also record or transmit images of your child via video or webcam, using video conferencing. We may also use videos for staff training and development. We may also wish to publish examples of pupils' work or the first names of pupils in specific school teams (images would not be published along with names).

I give consent for photographs and or videos of my child to be taken as a record of school events and visits

Yes □ No □

I give my consent for my child's image to be used in displays around the school. Yes □ No □

I give my consent for my child's image to be used on the school website and the school's social media accounts

Yes □ No □

I give my consent for my child's image to be used on other websites that promote St Bernadette's

Yes □ No □

I give my consent for my child's image to be used on the Tommy Flowers SCITT (teacher training provider based at St Paul's Catholic School, Milton Keynes) website.

Yes □ No □

I give my consent for my child's image to be used in the diocesan newspaper/ website.

Yes □ No □

I give my consent for my child's image to be used in other local press or publications promoting the school.

Yes □ No □

I give my consent for my child's image to be used in school newsletters, prospectus, leaflets or other printed publications that the school may produce for informative or promotional purposes.

Yes □ No □

I give consent for my child's first name to be published via the means mentioned above alongside examples of work or with reference to celebratory events (names will not appear alongside pupils' images).

Yes □ No □

As part of the curriculum, I give consent for my child's image to be transmitted via video or webcam, using video conferencing.

Yes □ No □

I give consent for my child's image to be used as part of staff training within St Bernadette's.

Yes □ No □

When/if working remotely, I give consent for my child to submit work activities involving their image to Google Classroom – the school's online learning platform

Yes □ No □

When/if working remotely, I give consent for my child to join live events such a remote assemblies, collective worship, services and peformances involving their image.

Yes □ No □

THE INTERNET

Internet access is part of the statutory curriculum. Pupils will be given clear objectives for Internet use and staff will select sites which will support the planned learning outcomes. Some of the material used in school will be on a cache system which means the children will not be live on the Internet. However, there may be occasions when direct access is required and it is for these occasions that we need your permission. Our Internet access provider operates a filtering system that restricts access to known inappropriate materials. Every endeavour will be made to ensure suitable restrictions are effective. However, neither the school nor Milton Keynes Council will be held responsible for the nature or content of material accessed through the Internet. Parents will be informed if any inappropriate material is viewed.

I give my permission for my child to access the Internet within school.

Yes □ No □

SCHOOL VISITS AND ACTIVITIES

Children will take part in activities offsite and sometimes outside school hours. These activities are planned to support the curriculum and/or to provide additional opportunities, which we hope your child will find helpful and enjoyable, e.g. visiting the locality, another school, museums, swimming lessons etc. Such visits and activities will be properly organised and all reasonable precautions will be taken for the safety and wellbeing of your child. Nevertheless, it is possible that your child may be exposed to additional hazards, e.g. accidents in the course of travel or sporting activities, when urgent medical treatment might be needed in circumstances where it is not possible to contact the parent/carer. In this situation, we hope you would be willing to agree that the teacher in charge of any party may give the necessary consent on your behalf. Please note that for longer trips parents will receive more detailed information and you will need to give specific written permission for these visits, separate from this form.

I give my consent for my child to participate in school visits/activities

Yes □ No □

I give my consent for members of staff to provide consent for any necessary urgent medical treatment to be administered when it is not possible to contact me.

Yes □ No □

MARKETING

I give consent for the school to send me marketing information by email promoting school events, campaigns, charitable causes or services that may be of interest to you.

Child's Name ..... (please print)

Parent's Name .....(Please print)

Signature ..... Date .....

Appendix 3

Staff Consent Form

Dear Staff,

The following information outlines activities for which we need to obtain your specific consent. Your consent will stand for the time you work at St Bernadette's or until legislation requires us to amend the details.

Staff members may withdraw consent at any time; this must be done formally in a letter addressed to the Headteacher. The Headteacher will respond in writing within two weeks of receipt of withdrawal of consent.

Please read each statement carefully and respond with either Yes or No to demonstrate whether you are or are not providing your permission, consent or agreement.

Yours faithfully

Mrs Zamora

(Headteacher)

STAFF MEMBER'S NAME .....

PHOTOGRAPHS and IMAGES

We like to take photographs of our staff and pupils which may be used for displays, as records of work/events, for publication in the diocesan/local press or on the school website, prospectus or other printed publications that the school may produce for informative or promotional purposes. As part of the Computing curriculum, we may also record or transmit images via video or webcam, using video conferencing. We also use videos for staff training and development (Iris Connect). We also display photographs of staff alongside their names in the main entrance of the school.

I give consent for photographs to be taken of me as a record of school events and visits

Yes □ No □

I give my consent for my image to be used in displays around the school.

Yes □ No □

I give my consent for my image to be used on the school website

Yes □ No □

I give my consent for my image to be used on other websites that promote St Bernadette's

Yes □ No □

I give my consent for my image to be used on the Tommy Flowers SCITT (teacher training provider based at St Paul's Catholic School, Milton Keynes) website.

Yes □ No □

I give my consent for my image to be used in the diocesan media and social media

Yes □ No □

I give my consent for my image to be used in other local press or publications promoting the school.

Yes □ No □

I give my consent for my image to be used in school newsletters, prospectus, leaflets or other printed publications that the school may produce for informative or promotional purposes.

Yes □ No □

I give consent for my name to be published via the means mentioned above alongside reports or with reference to celebratory events

Yes □ No □

I give consent for my name and image to be displayed in the board in the main school entrance

Yes □ No □

As part of the curriculum delivery, I give consent for my image to be transmitted via video or webcam, using video conferencing.

Yes □ No □

I give consent for my image to be used as part of staff training within St Bernadette's.

Yes □ No □

Name …… (please print)

Signature …… Date ……

CCTV

CCTV cameras are located on the external area of the school site and the reception area and are there to promote the safety and security of the school and the local community. They were upgraded in February 2018 on the advice of the police who, when responding to an incident in the locality, found that the images were unclear and therefore unhelpful in their investigation. We adhere to the ICO's code of practice for the use of CCTV. Security cameras are clearly visible and accompanied by prominent signs explaining that CCTV is in use. We do not need to ask individuals' permission to use CCTV.

Appendix 3

Data Breach Incident Report Form

Description of the Data Breach:	
Time and Date breach was identified and by whom.	
Who is reporting the breach: Name/Post/Dept	
Contact details: Telephone/Email	
Classification of data breached i. Public Data ii. Internal Data iii. Confidential Data iv. Highly confidential Data	
Volume of data involved	
Confirmed or suspected breach?	
Is the breach contained or ongoing?	
If ongoing what actions are being taken to recover the data	
Who has been informed of the breach	
Any other relevant information	