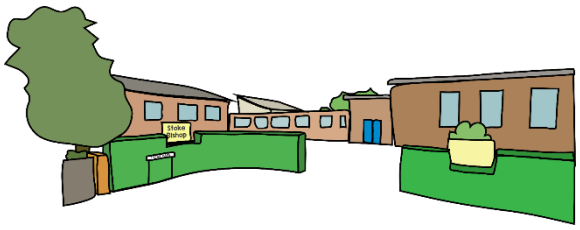
Stoke Bishop Church of England Primary School

Data Protection Policy



‘Believing it’s Possible’

Our community sits between two rivers that have historically supported growth and success. Working together with trust and passion, we learn, grow and thrive as we embrace the possibilities of life’s journey: Understanding that,

“Wherever the river flows, life will flourish” – Ezekiel 47:9

Reviewed by:	Leadership & Management Committee	Date: 26 March 2024
Approved by:	Leadership & Management Committee	Date: 26 March 2024
Next review due by:	March 2027 (or earlier if change in legislation or change in DPO)	

Contents

1. Aims

The Governors and Senior Leadership Team (SLT) of Stoke Bishop C of E Primary School are committed to ensuring that all personal data collected is processed in accordance with all relevant data protection laws including the General Data Protection Regulation (GDPR) and the Data Protection Act 2018 (DPA 2018).

The school is registered as a data controller with the Information Commissioner.

The details of the School's Data Protection Officer can be found at paragraph 6.

2. Scope

This policy applies to anyone who has access to and/or is a user of school ICT systems, both in and out of the School, including staff, governors, pupils, volunteers, parents / carers, visitors, contractors, and other community users.

The policy is also intended to serve as the Appropriate Policy Document for the processing of special category data and criminal record data (where applicable).

This policy applies to all personal data for which the school is the data controller, regardless of whether it is in paper or electronic format.

3. Distribution

This policy is available on the School website and in hard copy from the School office.

4. Definitions

Personal data - Any combination of data items which could identify a living person and provide specific information about them, their families or circumstances. The term covers both facts and opinions about an individual. The School may process a wide range of personal data of staff (including governors and volunteers) and pupils, their parents or guardians as part of its operation.

A non-exhaustive list of the types of personal data that we process may be found in our privacy notices.

Special category personal data – Formerly known as "sensitive personal data", special category data is information that is more sensitive and so needs more protection. These are:

- Racial or ethnic origin
- Political opinions
- Religious or philosophical beliefs
- Trade union membership

- Genetic data
- Biometric data (such as fingerprints, retina and iris patterns, voice biometrics), where used for identification purposes
- Health data – physical or mental
- Sex life or sexual orientation

Our Record of Processing Activities (RoPA) details the types of information we hold and the grounds upon which we process it, as do our Privacy Notices which may be found on our website. Examples of the types of special category data we process can be found at appendix 1.

Data subject - The data subject is the person about whom the personal data relates or identifies.

Data Processing – Data processing is the over-arching term that means "doing something" with personal data. This commonly includes:

- Collecting or collating the data;
- Analysing the data;
- Sharing the data;
- Storing the data;
- Destroying the data.

Data controller – The data controller is occasionally the person or more commonly the organisation with overall responsibility for the processing of personal data that the organisation undertakes. They will make all of the decisions about what is captured, how it's used and the purpose for it, as well as deciding what controls need to be in place.

Data processor – Is occasionally a person but more commonly an organisation commissioned by a data controller to carry out their data processing on behalf of the data controller. These are often software providers such as Microsoft or contracted out services such as an insurance company. Essentially, a data processor is acting as an extension of the data controller, so must operate under the data controller's instructions, and under the terms of a data processing agreement (contract).

Data Sharing – means giving data to another data controller, for them to use for their own purposes. Once you have shared personal data, the recipient becomes the data controller of that information and therefore makes the decisions over what they will do with it.

Note, we do not share ownership with our data processors, as they are processing it under our data controllership.

Data breach - The most common type of data breach is the accidental or unlawful *loss, alteration, destruction, disclosure of or access to* personal data, for example

sending an email to the wrong recipient, losing a file containing personal data, or sharing passwords enabling someone else to access your account. However, we consider any failing of one of the data protection principles (Article 5 of UK GDPR) as a breach of data protection legislation, so could include examples such as not having the necessary paperwork in place, not providing the data subject with clear privacy information, retaining personal data for longer than is necessary or processing personal data without an identified lawful basis (Article 6 of UK GDPR).

Data Processing Agreement – a legally binding contract between the data controller and its data processor. This contract defines exactly how the data controller expects the data processor to process its personal data and follow standard contract clauses.

Data Sharing Agreement - a non-legally binding written agreement between data controllers where there is regular sharing of personal data. The data sharing agreement should define who is involved in the agreement, what data is being shared, why the recipient needs the data, how this is lawful, how the data will be shared.

5. Roles and Responsibilities

Governing Body - The Governing Body has overall responsibility for ensuring that the School complies with all relevant data protection obligations.

The Data Protection Lead - acts with the delegated authority of the Governing Body on a day to day basis and will liaise with the DPO. This role is undertaken by the Headteacher, but this role can be delegated to the School Business Manager.

All other staff - All staff are responsible for:

- Familiarising themselves with and complying with this policy and related polices. The learning culture within the organisation seeks the avoidance of a blame culture and is key to allowing individuals the confidence to report genuine mistakes. However, staff should be aware, that a deliberate or reckless disregard of this policy could result in disciplinary action being taken;
- Taking care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse at all times. All staff should adopt the approach that they should treat the personal data of others with the same care with which they would treat their own;
- Only using computers and other devices authorised by the school for accessing and processing personal data ensuring that they are properly “logged-off” at the end of any session in which they are using personal data; and locking devices

when they are temporarily left unattended at any point (Windows button + L is a useful shortcut);

- Storing, transporting and transferring data using encryption and secure password protected devices;
- Not transferring personal data offsite or to personal devices, other than in accordance with our Bring Your own Device policy;
- Deleting data in line with this policy, the Records Management Policy and the retention schedule;
- Informing the School of any changes to their personal data, such as a change of address;
- Reporting to the Data Protection Lead, or in their absence the DPO in the following circumstances:
    - Any questions about the operation of this policy, data protection law, retaining or sharing personal data or keeping personal data secure;
    - If they have any concerns that this policy is not being followed;
    - If they are unsure whether they have a lawful basis upon which to use personal data in a particular way;
    - If they need to rely on or capture consent, deal with data protection rights invoked by an individual, or transfer personal data outside the UK and European Economic Area;
    - The discovery of a data breach or near miss (immediate action is required) – please refer to the Data Breach Policy and paragraph 12 of this policy;
    - Whenever they are engaging in a new activity that may affect the privacy rights of individuals;
    - If they are to share personal data with a data processor, for example a contractor or someone offering a service, in which case a contract is likely to likely to be required and potentially a data protection impact assessment (DPIA), please see - *Sharing Personal Data* (paragraph 10).

6. Data Protection Officer (DPO)

The Data Protection Officer (DPO) is responsible for advising on the implementation of this policy, monitoring compliance with data protection law, providing support and developing related policies and guidelines where applicable, in amongst other data protection related functions. They will provide an annual report on compliance directly to the Governing Body and, where relevant, provide the School with advice and recommendations on data protection issues.

The School has appointed One -West as its DPO, and they can be contacted by email at:

Email: i-west@bathnes.gov.uk.

Telephone: 01225 395959

One West
Bath and North East Somerset Council
Guildhall
High Street
Bath
BA1 5AW

Under usual circumstances the internal data protection lead, Headteacher or a member of SLT will be the point of contact with the DPO.

7. Data Subject Rights

In all aspects of its work, the School will ensure that the rights of the data subject are protected by all practicable measures associated with the conduct of the School's work. Subject to exceptions, the rights of the data subject as defined in law are:

a) The Right to be informed.

The School advises individuals how it will use their data through the use of transparent Privacy Notices and other documentation, such as data capture and consent forms where appropriate.

b) The Right of access

An individual when making a subject access request (SAR) is entitled to the following;

i. Confirmation that their data is being processed;
ii. Access to their personal data;
iii. Other supplementary information – this largely corresponds to the information that should be provided in a Privacy Notice.

The School must respond to such a request within one calendar month unless the request is complex, in which case it may be extended by a further 2 calendar months. Please refer to Appendix 2 for further details as to how to manage a subject access request.

c) The Right to rectification

Individuals have the right to ask us to correct information that they think is inaccurate or incomplete. The School has a duty to investigate any such claims and rectify the

information where appropriate within one calendar month, unless an extension of up to a further 2 calendar months can be justified.

d) The Right to erasure

Individuals have a right to request that their personal information is erased but this is not an absolute right. It applies in circumstances including where:

- The information was given voluntarily, consent is now withdrawn and no other legal basis for retaining the information applies;
- The information is no longer required;
- The data was collected from a child for an online service: or
- The data was collected from a child for an online service or
- The school has processed the data on the basis that it is in their legitimate business interests to do so, and having conducted a legitimate interests test, it concludes that the rights of the individual to have the data erased outweigh those of the School to continue to process it.

The School will consider such requests as soon as possible and within one month, unless it is necessary to extend that timeframe for a further two months on the basis of the complexity of the request or a number of requests have been received from the individual.

e) The Right to restrict processing

This is not an absolute right. An individual may ask the School to temporarily limit the use of their data (for example storing it but not using it) when we are considering:

- A challenge made to the accuracy of their data, or
- An objection to the use of their data.

An individual may also ask us to restrict the destruction of a record, if they wish it to be retained beyond the normal retention period.

In addition, the school may be asked to limit the use of data rather than delete it:

- If the individual does not want the School to delete the data but does not wish to it continue to use it;
- In the event that the data was processed without a lawful basis;
- To create, exercise or defend legal claims.

f) The Right to data portability

An individual can make a request in relation to data which is held electronically for it to be transferred to another organisation or to themselves where they have provided it either directly or through monitoring activities e.g. apps. The School only has to provide the information where it is electronically feasible.

g) The Right to object

Individuals have a right to object in relation to the processing of data in respect of:

- a task carried out in the public interest except where personal data is processed for historical research purposes or statistical purposes
- a task carried out for the exercise of official authority
- a task carried out in its legitimate interests
- scientific or historical research, or statistical purposes, or
- direct marketing.

Only the right to object to direct marketing is absolute, other objections will be assessed in accordance with data protection principles. The School will advise of any decision to refuse such a request within one month, together with reasons and details of how to complain and seek redress.

8. Data Protection Principles

The GDPR is based on 7 key data protection principles that the School complies with.

The principles say that personal data must be:

- **Processed lawfully, fairly and in a transparent manner** – the School will explain to individuals why the School needs their data and why it is processing it – for example on consent forms (where consent is used as the basis for processing), and in its Privacy Notices. The School reviews its documentation and the basis for processing data on a regular basis

- **Collected for specified, explicit and legitimate purposes** – the School explains these reasons to the individuals concerned when it first collects their data. If the School wishes to use personal data for reasons other than those given when the data was first obtained, it will inform the individuals concerned before doing so, and will seek consent where necessary and appropriate unless the new purpose is compatible with that in respect of which consent was given, or there is another lawful basis for sharing the information. The School will document the basis for processing.

- **Adequate, relevant and limited to what is necessary to fulfil the purposes for which it is processed -** the School must only process the minimum amount of personal data that is necessary in order to undertake its work.

- **Accurate and, where necessary, kept up to date** – the School will check the details of those on its databases at appropriate intervals and maintain the databases. It will consider and respond to requests for inaccurate data to be rectified in accordance with the Data Protection Act 2018.

- **Kept for no longer than is necessary for the purposes for which it is processed** – The school reviews what data we hold at appropriate intervals – for example upon the annual review of the Record of Processing Activities (or sooner if needed). When the School no longer needs the personal data it holds, it will ensure that it is deleted or anonymised in accordance with the retention schedule. The school only keeps personal data, include special category data in an identifiable form for as long as is necessary for the purposes for which it was collected, or where there is a legal obligation to do so;

    - The school has a Records Management policy which governs how long all data including special category data shall be retained for. This policy is complied with and reviewed regularly;
    - Once the data is no longer needed, the school deletes it, securely destroys it in line with our Records Management policy, or renders it permanently anonymous.

- **Processed in a way that ensures it is appropriately secure** – the School implements appropriate technical measures to ensure the security of data and systems for staff and all users. Please refer to the Information Security Policy and Online Safety Policy, which incorporates principles around Bring your Own Device (BYOD).

- **Accountability –** The School complies with its obligations under data protection laws including the GDPR and can demonstrate this via the measures set out in this policy including:

- completing data protection impact assessments (DPIAs) where necessary; integrating data protection into internal documents including this policy, any related policies and privacy notices; regularly training members of staff on all relevant data protection law, including this and any related policies; reviewing and auditing privacy measures and compliance; maintaining and reviewing records of its processing activities for all personal data that it holds; reviewing and ensuring familiarity of policies related to the handling of data; reviewing reasons for data breaches; and ensuring stakeholders manage risks and compliance using the risk register.

9. Processing Personal Data

In order to ensure that the School's processing of personal data is lawful; it will always identify one of the following six grounds for processing **before** starting the processing:

- The data needs to be processed so that the School can fulfil a **contract** with the individual, or the individual has asked the School to take specific steps before entering into a contract;
- The data needs to be processed so that the school can comply with a **legal obligation;**
- The data needs to be processed to ensure the **vital interests** of the individual e.g. to protect someone's life;
- The data needs to be processed so that the School, as a public authority, can **perform a task in the public interest, and carry out its official functions**;
- The data needs to be processed for the **legitimate interests** of the School or a third party where necessary, balancing the rights of freedoms of the individual).
- However, where the School can use the public task basis for processing, it will do so rather than rely on legitimate interests as the basis for processing.
- The individual (or their parent/carer when appropriate in the case of a pupil) has freely given clear consent. The School will seek consent (where appropriate) to process data from the pupil or parent depending on their age and capacity to understand what is being asked for.

Processing Special Categories of Personal Data

In addition to the legal basis to process personal data, special categories of personal data also require an additional condition for processing under Article 9 of the GDPR. The grounds that we may rely on include:

a) The individual has given **explicit consent** to the processing of those special categories of personal data for one or more specified purposes;

b) Processing is necessary for the purposes of carrying out the obligations and exercising specific rights under **employment, health and social security and social protection law and research**; a full list can be found in Schedule 1 Part 1 of the Data Protection Act 2018.

c) Processing is necessary to protect the **vital interests** of the individual or of another natural person where the individual is physically or legally incapable of giving consent;

d) Processing relates to personal data which are manifestly **made public** by the individual;

e) Processing is necessary for the **establishment, exercise or defence of legal claims** or whenever courts are acting in their judicial capacity;

f) Processing is necessary for reasons of **substantial public interest** but must be clearly demonstrated and assessed as part of the public interest test and evidenced throughout the decision- making process.

These grounds include the following (the full list of defined purposes may be found in Schedule 1 Part 2 of the Data Protection Act 2018):

- Statutory and government purposes
- Safeguarding of children or individuals at risk
- Legal claims
- Equality of opportunity or treatment
- Counselling
- Occupational pensions

g) Processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in paragraph 3 ;

h) Processing is necessary for reasons of **public interest in the area of public health;**

i) Processing is necessary for **archiving purposes in the public interest, scientific or historical research purposes or statistical purposes**.

Deciding upon the correct legal basis for processing data can be difficult and more than one ground may be applicable. We consult with the Data Protection Officer where appropriate.

We must also comply with Schedule 1 of the Data Protection Act (as well as Articles 6 and Article 9), when we are processing data where the conditions relate to employment, health and research or substantial public interest as follows:

Legal basis for processing criminal offence data

Criminal offence data includes information about criminal allegations, criminal offences, criminal proceedings and criminal convictions.

We do not maintain a register of criminal convictions.

When processing this type of data, we are most likely to rely on one of the following bases:

- The processing is necessary for the purposes of performing or exercising obligations or rights which are imposed or conferred by law on the controller

or the individual in connection with employment, social security or social protection;

- The processing is necessary for the purposes of protecting the physical, mental or emotional wellbeing of an individual:
- The processing is necessary for statutory purposes: or
- Consent – where freely given. The School acknowledges because of the potential for the imbalance of power that it may be difficult for consent to be deemed valid and will only rely on this where no other ground applies.

Third Parties with Access to Personal Data

Please refer to the School's Privacy Notices for details of who, aside from the school, has access to the personal data processed.

Data Sharing

- The School will only share personal data under limited circumstances, when there is a lawful basis to do so and where identified in the Privacy Notices. The following principles apply:
    - The School will share data if there is an issue with a pupil or third party, for example, parent/carer that puts the safety of staff or others at risk; The School will share data where there is a need to liaise with other agencies. It will seek consent as necessary and appropriate before doing so. However, where child protection and safeguarding concerns apply, it will apply the "Seven golden rules of information sharing" which provide that in limited circumstances data may be shared with external agencies without the knowledge or consent of the parent or child in line with the DPA 2018, which includes "safeguarding of children and individuals at risk as a condition that allows practitioners to share information without consent;

We may also disclose personal data to law enforcement and government bodies where there is a lawful requirement / basis for us to do so, including:

- For the prevention or detection of crime and/or fraud;
- For the apprehension or prosecution of offenders;
- For the assessment or collection of tax owed to HMRC;
- In connection with legal proceedings;
- For research and statistical purposes, as long as personal data is sufficiently anonymised, or consent has been provided or it is otherwise fair and lawful to do so.

We may also share personal data with emergency services and local authorities to help them to respond to an emergency situation.

Third Party Processors

The School's suppliers and contractors including its data protection officer and IT services provider may need data to provide services. When sharing data, the School will:

- Only appoint suppliers or contractors which can provide sufficient guarantees that they comply with data protection law;
- Establish a data processing 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 it shares where there is regular sharing;
- Only share data that the supplier or contractor needs to carry out their service, and information necessary to keep them safe while working with the School.

- The School may also share personal data with law enforcement and government bodies where there is a lawful requirement / basis for us to do so, including:
  - For the prevention or detection of crime and/or fraud;
  - For the apprehension or prosecution of offenders;
  - For the assessment or collection of tax owed to HMRC;
  - In connection with legal proceedings;
  - For research and statistical purposes, as long as personal data is sufficiently anonymised, or consent has been provided.

10. Data Protection by Design and Default

The School has a legal obligation to integrate appropriate technical and organisational measures into all of its processing activities, and to consider this aspect before embarking on any new type of processing activity.

It is a statutory requirement that any activity involving a high risk to the data protection rights of the individual when processing personal data be assessed by the Data Protection Impact Assessment. Prior to the assumption of any such activity One West must be consulted and an initial screening be conducted assessing risk.

Please refer to the Information Security Policy for further detail as to how the School implements this principle in practice.

11. Personal data breaches or near misses

A personal data breach is defined as *"a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed in connection with the provision of a public electronic communications service."* It may be deliberate or accidental.

Wherever it is believed that a security incident has occurred or a 'near miss' has occurred, the staff member must inform the Data Protection Lead who will inform the DPO **immediately** in order that an assessment can be made as to whether the ICO should be informed within 72 hours as is legally required, and / or those data subjects affected by the breach. The learning culture within the organisation seeks the avoidance of a blame culture and is key to allowing individuals the confidence to report genuine mistakes.

Further details on security incidents and data breaches can be found in the Data Breach Policy.

12. Destruction of records

The School adheres to its Records Management policy and will permanently securely destroy both paper and electronic records securely in accordance with these timeframes.

The School will ensure that any third party who is employed to perform this function has the necessary accreditations and safeguards.

Where the School deletes electronic records and its intention is to put them beyond use, even though it may be technically possible to retrieve them, it will follow the Information Commissioner's Code of Practice on deleting data and this information will not be made available on receipt of a subject access request.

13. Training

To meet its obligations under Data Protection legislation, the School will ensure that all staff, volunteers, and Governors receive an appropriate level of data protection training as part of their induction. Those who have a need for additional training will be provided with it.

Data protection also forms part of continuing professional development, and updates will be provided where changes to legislation, guidance or the School's processes make it necessary.

14. Monitoring Arrangements

Whilst the DPO is responsible for advising on the implementation of this policy and monitoring the School's overall compliance with data protection law, the School is responsible for the day to day implementation of the policy and for making the data protection officer aware of relevant issues which may affect the School's ability to comply with this policy and the legislation.

This policy will be reviewed every three years, unless an incident or change to regulations dictates a sooner review.

15. Complaints

The School is always seeking to implement best practice and strives for the highest standards. The School operates an "open door" policy to discuss any concerns about the implementation of this policy or related issues. The School's complaints policy may be found on its website.

There is a right to make a complaint to the Information Commissioner's Office (ICO), but under most circumstances the ICO would encourage the complainant to raise the issues in the first instance with the School or via the School's DPO.

The ICO is contactable at:

Wycliffe House,
Water Lane,
Wilmslow,
Cheshire,
SK9 5AF.

Telephone: 0303 123 1113.

16. Legislation and Guidance

This policy takes into account the following:

- The General Data Protection Regulation (GDPR) 2018
- The Data Protection Act (DPA) 2018.
- The Protection of Freedoms Act 2012
- Guidance published by the Information Commissioner's Office
- Information Sharing – Advice for Practitioners – DfE July 2018.

17. Links with Other Policies

This Data Protection Policy is linked to the following:

- Information Security Policy
- Records Management Policy
- Data Breach Policy
- Privacy Notices
- Child Protection and Safeguarding Policy
- Online Safety Policy
- Consent / Permissions Forms
- Admissions Forms

Appendix 1 – Examples of Special Category Data that we process

Examples of where we may process special category data include in:

- Employee health data and information concerning their racial / ethnic origin
- Pupil health data and information concerning their racial / ethnic origin in admissions records and in pupil records / trip packs
- Special educational needs information
- School census information
- Attendance records
- Information contained within child protection and safeguarding records
- Staff application forms
- HR files including disciplinary and capability proceedings which may include DBS, and right to work checks, health, and equal opportunities data (disability, race, ethnicity, sexual orientation).
- Accident reporting documentation

Our Record of Processing Activities (RoPA) details the types of information we hold and the grounds upon which we process it, as does our Privacy Notice which may be found on our website.

Appendix 2 – Subject Access Request Procedure (SAR)

The school shall complete the following steps when processing a request for personal data (Subject Access Request or SAR) with advice from its Data Protection Officer (i-west), using the School SAR Guidance provided to the school.

1. Ascertain whether the requester has a right to access the information and capacity.

2. Obtain (reasonable and proportionate) proof of identity

3. Engage with the requester if the request is too broad or needs clarifying (once steps 2 and 3 have been completed the "clock" can start)
4. Make a judgement on whether the request is complex and therefore can be extended by an additional 2 months

5. Acknowledge the requester providing them with
    a. the response time – 1 calendar month (as standard), an additional 2 months if complex; and
    b. details of any costs – Free for standard requests, or you can charge, or refuse to process if the request is manifestly unfounded or excessive, or further copies of the same information is required, the fee must be in line with the administrative cost

6. Use its Record of Processing Activities and/or data map to identify data sources and where they are held

7. Collect the data (the organisation may use its IT support to pull together electronic data sources such as emails and databases.)

8. If (6) identifies third parties who process it, then engage with them to release the data to the school.

9. Review the identified data for exemptions and redactions in line with the ICO's Guide to the Right of Access and in consultation with the organisation's Data Protection Officer (One West).

10. Create the final bundle and check to ensure all redactions have been applied

11. Submit the final bundle to the requester in a secure manner and in the format they have requested.