St Mary's C of E (Aided) Primary School

Headteacher
Mrs Yvonne Stallwood-Barnes
BEd(Hons) NPQH

Excellence • Equality • Encouragement

St Mary's C of E (Aided) Primary School
The Green
Chipping Norton
Oxfordshire
OX7 5DH

Data Protection Policy and Procedures

Reviewed: November 2020
Governors: 25 November 2020
Next review date: November 2021

Contents

1. Aims

This policy, along with accompanying procedures and associated policies, sets out our school's commitment to safe data protection practice.
It applies to all personal data, regardless of whether it is in paper or electronic format and includes an individual's right to access information about themselves and disclosure of information.

It is reviewed annually and updated in line with any changes to data protection legislation.

2. Legislation and Guidance

This policy meets the requirements of the General Data Protection Regulation (GDPR) and the provisions of the UK's Data Protection Act 2018.

3. Contact

If you would like to discuss anything in this policy, in the first instance please contact our Headteacher or Data Protection Officer (DPO) as follows:

Headteacher – Yvonne Stallwood-Barnes

DPO - nicola@schoolsdpo.com

4. Definitions

Term	Definition
Personal data	Data from which a person can be identified (i.e. distinguished from other individuals); such as: ● Name (including initials) ● Identification number ● Location data ● email address, telephone number, car registration number ● Online identifier, such as a username, IP addresses, cookie identifiers ● photographs, video recordings This includes data that, when combined with other readily available information, leads to a person being identified.

Special category personal data	Personal data which is more sensitive and is therefore afforded more protection under the GDPR. Data such as: ● Racial or ethnic origin ● Political opinions ● Religious beliefs, or philosophical beliefs ● Where a person is a member of a trade union ● genetic data ● biometric data (when used for identification purposes) ● Physical and mental health ● Sexual orientation and sex life Data relating to criminal convictions is afforded similar special protection.
Processing	Any operation carried out on personal data, such as collecting, recording, storing, altering, retrieving, using, disseminating, erasing or destroying. Processing can be automated or manual.
Data subject	The living individual whose personal data is held or processed
Data controller	A person or organisation that determines the purpose for which, and the way personal data is processed
Data processor	A person, or other body, other than an employee of the data controller, who processes the 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. Breaches can be the result of accidental or deliberate causes.

5. The Data Controller

Our school processes personal information relating to students, staff, parents, students' emergency contacts and visitors, and, therefore, is a data controller.

We are registered as a data controller with the Information Commissioner's

Office and our registration is renewed annually.

6. Roles and Responsibilities

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

The **Headteacher** has overall responsibility for ensuring the implementation of this policy. They will ensure that all staff are aware of their data protection obligations, and oversee any queries related to the storing or processing of personal data.

The **Data Protection Officer** monitors compliance with data protection law, providing support and guidance as required.

All Staff

All Staff are responsible for ensuring that they process any personal data in accordance with this policy (a definition of processing can be found in section 4). Staff must also inform the office of any changes to their personal data, such as a change of address.

Staff must contact the office whenever they have a query about data protection, including, but not limited to the following:

- any questions about the operation of this policy: including retaining personal data; keeping personal data secure; sharing personal data with third parties; or whether there is a lawful basis in place for a particular data processing operation
- any concerns that the policy is not being followed
- a new project under consideration that involves the processing of personal data
- received any requests from individuals for access to their personal information the Trust is processing.

7. Data Protection Principles

The GDPR is based on the following data protection principles, or rules for good data handling:

- Data shall be processed lawfully, fairly and in a transparent manner in relation to individuals
- collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered

to be incompatible with the initial purposes

- adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed
- accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay
- kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed. Personal data may be stored for longer periods, insofar as the personal data will be processed solely for archiving purposes in the public interest; scientific or historical research purposes or statistical purposes. This is subject to implementation of the appropriate technical and organisational measures required by the GDPR, in order to safeguard the rights and freedoms of individuals
- 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 GDPR also requires data controllers to be able to demonstrate their compliance under the principle of accountability.

This Data Protection Policy, along with our privacy notices and additional policies and procedures referenced in section 19, sets out how we aim to comply with these principles.

Lawfulness

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

- 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
- data needs to be processed so that the school can comply with a l**egal obligation**
- data needs to be processed to ensure the **vital interests** of the individual, e.g. to protect someone's life
- 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
- data needs to be processed for the **legitimate interests** of the school or a third party (provided the individual's rights and freedoms are not overridden)
- The individual (or their parent/carer when appropriate in the case of a pupil) has freely given clear **consent**

For **special categories** of personal data, we will also meet one of the special category conditions for processing set out in the GDPR:

- Explicit consent
- Employment, social security and social protection (if authorised by law)
- Vital interests
- Not-for-profit bodies
- Made public by the data subject
- Legal claims or judicial acts
- Reasons of substantial public interest (with a basis in law)
- Health or social care (with a basis in law)
- Public health (with a basis in law)
- Archiving, research and statistics (with a basis in law).

If we are relying on one of the special category conditions for our data processing which has a basis in law or is required by law, we will also meet one of the additional conditions as required by Section 10 of the UK DPA 2018.

Fairness and transparency

Our Pupil and Parent Privacy Notice sets out how we process personal data to support teaching and learning, to provide pastoral care and to assess the performance of our services.

Our Staff Privacy Notice sets out how we process staff personal data to fulfil our obligations as an employer.

Both Privacy Notices also include information on the rights of the individuals whose data we are processing and who to contact to discuss any aspect further.

Whenever we first collect personal data directly from individuals, we will provide them with the relevant information required by data protection law. This will normally be through our privacy notices.

Purposes

We will only collect personal data for specified, explicit and legitimate reasons. We will explain these reasons to 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 identify and document a new lawful basis, although this may not be necessary if our new purpose is compatible with the original purpose. We will inform the individuals concerned before we do so and seek consent where necessary.

Limitation, minimisation and accuracy

Staff will only process personal data where it is necessary in order to perform their roles.

When our school no longer needs the personal data it is processing, it will be deleted or anonymised. This will be done in accordance with our data retention schedule.

Data held will be as accurate and up to date as is reasonably possible. If a data subject

informs us of a change of circumstances, his/her records will be updated as soon as is practicable.

Where a data subject challenges the accuracy of his/her data, we will immediately mark the record as potentially inaccurate, or "challenged".

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.

All members of staff are required to sign an acceptable user agreement.

In particular:

- Paper-based records and portable electronic devices, such as laptops and hard drives, that contain personal information are kept securely when not in use
- Papers containing confidential personal information are not left on office and classroom desks, on staff room tables, pinned to notice/display boards, or left anywhere else where there is general access
- Where personal information needs to be taken off site (in paper or electronic form), staff must sign it in and out from reception
- Staff must adhere to our policies and procedures when taking data off site and when working remotely or at home
- Passwords that are at least 8 characters long containing letters and numbers are used to access academy systems, online resources, laptops and other electronic devices. Encryption software is used to protect all portable devices and removable media
- Staff should not store personal information on their personal devices and are expected to follow the same security procedures as set out for any Tutorial Foundation owned equipment.
- GDPR compliant cloud storage will be used for all online data storage
- The use of USB devices is not allowed.

8. Disposal of Records

Personal information that is no longer needed, or has become inaccurate or out of date, is disposed of securely.

For example, we shred or incinerate paper-based records, and overwrite or delete electronic files. We also use an outside company to convert paper records to electronic and to shred documents on site.

9. Accountability

The school has put in place appropriate technical and organisational measures to meet the

requirements of accountability. These include:

- The appointment of a data protection officer who reports directly to our highest management level
- Taking a 'data protection by design and default' approach to our activities
- Maintaining accurate documentation of our processing activities, such as the purposes of processing personal data, data sharing and retention. We also document the lawful bases we are relying on for our purposes, including how and when consent was obtained, as appropriate
- Adopting and implementing data protection policies and ensuring we have written contracts in place with our data processors
- Implementing appropriate security measures in relation to the personal data we process
- Carrying out data protection impact assessments for our high-risk processing (see section 10).

We regularly review our accountability measures and update or amend them when required.

10. Data Protection Impact Assessments

The GDPR requires us to carry out Data Protection Impact Assessments (DPIAs) for any type of processing that is likely to result in a high risk to individuals' interests; for example, when introducing new technologies, or using biometric data for identification purposes.

To assess the level of risk, we consider both the likelihood and the severity of any impact on individuals. High risk can result from either a high probability of some harm, or a lower possibility of serious harm.

If we identify a high risk that we cannot mitigate, we will consult the ICO before starting the processing.

As part of our data protection by design and default approach we will carry out a DPIA for any other major project which requires the processing of personal data.

We follow the ICO's guidelines and our DPIAs:

- describe the nature, scope, context and purposes of the processing
- assess necessity, proportionality and compliance measures
- identify and assess risks to individuals
- identify any additional measures to mitigate those risks.

11. Sharing Personal Data

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

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

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

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

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

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

Where we share personal data on an ad hoc or 'one off' basis, we will record the details including our purpose and lawful basis for doing so.

12. Subject Access Requests

Under the GDPR, staff, students and parents\carers have a right to make a 'subject access request' to gain access to information the Trust holds about them. This includes:

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

- Whether any automated decision-making is being applied to their data, and what the significance and consequences of this might be for the individual

Subject access requests can be made by contacting any member of staff, but it is helpful if they are made to the School Office or the DPO. They can be made in person, verbally, in writing, and by email. The following information will be required:

- Name of individual
- Relationship of the requester to the individual, if appropriate
- Correspondence address
- Contact number and email address
- Details about the information requested

If a member of staff receives a subject access request, they must immediately forward it to the School Office.

Members of staff can find further information on their role in handling subject access requests in our Guidance for Staff.

Children and subject access requests

A child's personal data always belongs to them rather than 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.

The Information Commissioner's Office, the organisation that upholds information rights, generally regards children aged 12 and above as mature enough to understand their rights and the implications of a subject access request. However, we will always consider this on a case by case basis.

Responding to subject access requests

When responding to requests, we:

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

We will not reveal the following information in response to Subject Access Requests:

- Information that might cause serious harm to the physical or mental health of the subject or another individual

- Information that would reveal that the child is at risk of abuse, where disclosure of that information would not be in the child's best interests
- Information contained in adoption and parental order records
- Certain information given to a court in proceedings concerning the child
- Any references that have been provided in confidence.

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

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

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

13. 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 6), individuals also have the right to:

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

If staff receive such a request, they must immediately forward it to the school office.

14. Parental Requests to access their Child's Educational Record

In maintained schools, parents have a separate right to access their child's educational

record under the Education (Pupil Information, England) Regulations 2005. The request must be made in writing and the information will be provided within 15 school days of receipt of the request.

15. Photos and Videos

As part of our educational activities, we may take photographs and record images of individuals. We will always clearly explain to pupils and/or parents (as appropriate) how the photograph or video will be used.

We will obtain consent for photographs and videos to be taken of pupils for communication, marketing and promotional materials.

Uses may include:

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

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 individual, to ensure they cannot be identified.

See our Child Protection and Safeguarding Policy for more information on our use of photographs and videos.

16. Personal Data Breaches

The GDPR defines a personal data breach as a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

This includes breaches that are the result of both accidental and deliberate causes. It also means that a breach is more than just about losing personal data.

Personal data breaches can include:

- access by an unauthorised third party
- deliberate or accidental action (or inaction) by a controller or processor
- sending personal data to an incorrect recipient
- computing devices containing personal data being lost or stolen
- alteration of personal data without permission
- loss of availability of personal data.

When a personal data breach has occurred, we will assess the likelihood and severity of the resulting risk to the rights and freedoms of the individuals involved. If it's likely that there will be a risk, then we are required by law to notify the ICO.

Data Breach Register

We record all breaches of personal data regardless of whether they are reported to the ICO. Our academy data breach registers include the details of the breach, its effects and any remedial action taken. Remedial action may include a review of relevant systems or policies and procedures; additional training for staff; or other corrective steps, as appropriate.

Data Breach Response Plan

Each breach will be considered on a case by case basis and our Data Breach Response Plan sets out in more detail the procedures we will follow.

If any member of staff believes a breach of personal data has occurred or might have occurred they are required to let the headteacher know immediately.

17. Training

Our staff are provided with data protection training as part of their induction process and this is refreshed at least annually.

Data protection also forms part of continuing professional development, where changes to legislation or our data processing make it necessary. Uptake of training is monitored and procedures are in place to ensure that all staff complete the required training.

18. Monitoring Arrangements

The Governing Board is responsible for monitoring and reviewing this policy. It will be reviewed on an annual basis.

19. Links with other policies and procedures

This Data Protection Policy is linked to:

- Privacy Notice (Pupil and Parent/Carer)
- Privacy Notice (Staff)
- Record Retention Schedule
- Guidance for Staff on Subject Access Requests

- Data Breach Response Plan
- Child Protection Policy/Safeguarding Policy
- Freedom of Information Publication Scheme.