Document Ref	Doc-01-06
Version	1.1
Date	05/11/2018
Author	Mark McGeown
Last review date	N/A
Next review due by	31/10/2019

ST WERBURGH'S PRIMARY SCHOOL

DATA PROTECTION POLICY

St Werburgh's Primary School (the School) collects and uses personal information about staff, pupils, parents and other individuals who come into contact with the school. This information is gathered in order to enable it to provide education and other associated functions. In addition, there may be legal requirements to collect and use information to ensure that the School complies with its statutory obligations.

The School is registered as a Data Controller with the Information Commissioner's Office (ICO) detailing the information held and its use.

This policy is intended to ensure that personal information is dealt with correctly and securely and in accordance with the EU General Data Protection Regulation 2016 and the Data Protection Act 2018. It will apply to information regardless of the way it is collected, used, recorded, stored and destroyed, irrespective of whether it is held in paper files or electronically.

Table of Contents

1. Definitions

We have set out below the key definitions that are contained within the General Data Protection Regulation (GDPR) and the Data Protection Act 2018 (DPA). You will find this useful in understanding their meaning and effect when interpreting your rights and our obligations under the GDPR and DPA.

Term	Definition
Personal data	Any information relating to an identified, or identifiable, individual. This may include the individual's: • name (including initials) • identification number • location data • online identifier, such as a username It may also include factors specific to the individual's physical, physiological, genetic, mental, economic, cultural or social identity.
Special categories of personal data	Personal data which is more sensitive and so needs more protection, including information about an individual's: • racial or ethnic origin • political opinions • religious or philosophical beliefs • trade union membership • genetics • biometrics (such as fingerprints, retina and iris patterns), where used for identification purposes • health – physical or mental • sex life or sexual orientation
Processing	Anything done to personal data, such as collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing or destroying. Processing can be automated or manual.
Data subject	The identified or identifiable individual whose personal data is held or processed.
Data controller	A person or organisation that determines the purposes and the means of processing of personal data.
Data processor	A person or other body, other than an employee of the data controller, who processes personal data on behalf of the data controller.
Personal data breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.

2. The Data Controller

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

3. Roles and Responsibilities

This policy applies to all staff employed at the School, and to external organisations or individuals working on our behalf.

3.1 Governing Body

The governing body has overall responsibility for ensuring that the School complies with all relevant data protection obligations.

3.2 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 is also the first point of contact for individuals whose data the School processes, and for the ICO. Our DPO is Bristol City Council Office of Data Protection, contactable at City Hall, College Green, Bristol, BS1 5TR, odp.schools@bristol.gov.uk.

3.3 Head-teacher

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

3.4 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 they have a lawful basis to use personal data in a particular way;
    - if they need to rely on or capture consent, draft a privacy notice, deal with data protection rights invoked by an individual, or transfer personal data outside the European Economic Area;
    - if there has been a data breach;
    - whenever they are engaging in a new activity that may affect the privacy rights of individuals;
    - if they need help with any contracts or sharing personal data with third parties.

4. Data Protection Principles

The GDPR is based on data protection principles that the 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 fulfill 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.

5. Collecting Personal Data

5.1 Lawfulness, Fairness And Transparency

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

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

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

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

5.2 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.

6. 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 who 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, if 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 that affects any of our pupils or staff.

7. Subject Access Requests And Other Rights Of Individuals

7.1 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 is not possible, the criteria used to determine this period;
- the source of the data, if not the individual;
- whether any automated decision-making is being applied to their data, and what the significance and consequences of this might be for the individual.

Subject access requests should include the following:

- the individual's name;
- the individual's correspondence address;
- the individual's 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.

7.2 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, or be aged 13 and under.

7.3 Responding To Subject Access Requests

When responding to requests, we:

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

We will not disclose information if it:

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

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

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

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

7.4 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 do the following:

- to withdraw their consent to processing at any time;
- to ask the School to rectify, erase or restrict processing of their personal data, or object to the processing of it (in certain circumstances).
- to prevent use of their personal data for direct marketing;
- to challenge processing that has been justified on the basis of public interest;
- to request a copy of agreements under which their personal data is transferred outside of the European Economic Area;
- to object to decisions based solely on automated decision making or profiling (decisions taken with no human involvement, that might negatively affect them);
- to prevent processing that is likely to cause damage or distress;
- to be notified of a data breach in certain circumstances;
- to make a complaint to the ICO;
- to 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.

8. 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.

9. Biometric Recognition Systems

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

Parents/carers will be notified before any biometric recognition system is put in place or before their child first takes part in it. The School will obtain written consent from at least one parent or carer any biometric data is taken from their child and processed for the first time.

Parents/carers and pupils have the right to choose not to use any biometric system(s) introduced by the School. The School would provide alternative means of accessing the relevant services for those pupils. In the example above, pupils would be able to pay for school dinners in cash at each transaction if they wished.

Parents/carers and pupils can object to participation in any biometric recognition system or systems introduced by the School, or withdraw consent at any time, and the School would make sure that any relevant data that had already been captured would be deleted.

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

Where staff members or other adults used a biometric system or systems introduced by the School, their consent would be obtained before they first took part in it; and the School would provide alternative means of accessing the relevant service if they objected. Staff and other adults would be able to withdraw consent at any time, and the School would delete any relevant data it had already captured.

10. CCTV

The School uses CCTV in various locations around its two sites to ensure that it remains safe.

The School does not need to ask individuals' permission to use CCTV, but it does make it clear in which locations 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 in the first place to the School Administrator.

11. 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 parents/carers.

Uses may include:

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

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

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

12. Data Protection by Design and Default

We will put measures in place to show that we have integrated data protection into all our data processing activities. Specifically, the School will ensure the following:

- that a suitably qualified DPO is appointed, and that he/she has the necessary resources to fulfil their duties and maintain their expert knowledge;
- that it processes only the personal data necessary for each specific purpose of processing, and that it is remains in line with the data protection principles set out in relevant data protection law (see section 6);
- that it carries out privacy impact assessments where its processing of personal data presents a high risk to rights and freedoms of individuals, and when any new technologies are introduced (the DPO will advise on this process);
- that the principles and provisions of data protection are integrated into the School's internal documents, including this data protection policy document, and any related policies and privacy notices;
- that members of staff receive regular training on data protection law, this data protection policy and any related policy documents, and any other areas related to data protection. We will also maintain records of such training;
- reviews and audits are carried out regularly to test the School's privacy measures and make sure that the School remains compliant;
- maintaining records of our processing activities, including:
    - for the benefit of data subjects, making available the name and contact details of our school and DPO; the information we are required to share; information on how we use and process such personal data (via our privacy notices);
    - for all personal data that we hold, maintaining an internal record of the type of data; the data subject; how and why we are using the data; any third-party recipients; how and why we are storing the data; the periods for which we retain personal data; and how we keep the data secure.

13. 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, we will ensure that:

- all paper-based records and portable electronic devices, such as laptops and hard drives that contain personal data are kept under lock and key when not in use;
- staff do not leave papers containing confidential personal data on office and classroom desks, on staffroom tables, pinned to notice/display boards, or anywhere else where there is general access;
- staff protect personal data when it needs to be taken off site, by signing it in and out from the school office;
- all school computers, laptops and other electronic devices are password protected and that staff and pupils, if appropriate, are reminded to change their passwords at regular intervals;
- any staff or governors, if appropriate, who store personal information on personal devices follow the same security procedures as for school-owned equipment;

- where we need to share personal data with a third party, we will carry out due diligence and take reasonable steps to ensure it is stored securely and adequately protected (see section 8).

14. 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.

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.

15. 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 below in Appendix 1.

16. Training

All current and new staff and governors will be provided with data protection training as part of their induction process and general GDPR awareness.

17. Monitoring Arrangements

The DPO is responsible for monitoring and reviewing this policy.

This policy will be reviewed annually an updated, if necessary, to comply with requirements of the EU GDPR and or the Data Protection Act 2018.

18. Links with other Policies

This data protection policy is linked to other policies that we may implement from time to time, such as the School's E-Safety Policy.

Appendix 1: Personal Data Breach Procedure

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

1. If a data processor or other member of staff causes a data breach or potential breach, or discovers that a data breach or potential breach has occurred, he/she must notify the School's Data Protection Officer (DPO) immediately and report it.

2. The DPO will investigate the report and determine whether a breach has occurred. In order to make the decision, 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, or
- made available to unauthorised people.

3. The DPO will alert the Head-Teacher and the Chair of Governors.

4. The DPO will make all reasonable efforts to contain and minimise the impact of the breach, assisted by relevant staff members or data processors where necessary.

5. The DPO will assess the potential consequences, based on how serious they are, and how likely they are to happen.

6. The DPO will determine whether the breach must be reported to the ICO. This must be judged on a case-by-case basis. To decide, the DPO will consider whether the breach is likely to negatively affect people's rights and freedoms, and cause them any physical, material or non-material damage (e.g. emotional distress), including through:

- loss of control over their data,
- discrimination,
- identify theft or fraud,
- financial loss,
- unauthorised reversal of pseudonymisation (for example, key-coding),
- damage to reputation,
- loss of confidentiality,
- any other significant economic or social disadvantage to the individual(s) concerned.

7. If it is likely that there will be a risk to people's rights and freedoms, the DPO must notify the ICO.

8. The DPO will ensure that a record of security breaches is maintained and he/she will document all decisions taken in respect of the management and conduct of such breaches.

9. Where the ICO must be notified, the DPO will do this via the 'report a breach' page of the ICO website within 72 hours. As required, the DPO will set out:

- a description of the nature of the personal data breach, including, where possible:
    - the categories and approximate number of individuals concerned;
    - the categories and approximate number of personal data records concerned.
- the name and contact details of the DPO;
- a description of the likely consequences of the personal data breach;
- a description of the measures that have been, or will be taken, to deal with the breach and mitigate any possible adverse effects on the individual(s) concerned.

10. If all the above details are not known, the DPO will report as much as possible 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.

11. The DPO will also assess the risk to individuals; again based on the severity and likelihood of potential or actual impact. If the risk is high, the DPO will inform in writing, promptly, any individuals whose personal data has been breached. This notification will set out:

- the name and contact details of the DPO;
- a description of the likely consequences of the personal data breach;
- a description of the measures that have been taken, or will be taken, to deal with the data breach and mitigate any possible adverse effects on the individual(s) concerned.

12. The DPO will notify any relevant third parties who can help mitigate the loss to individuals – for example, the police, insurers, banks or credit card companies.

13. The DPO will document each data breach reported to him/her, irrespective of whether it is subsequently reported to the ICO. For each data breach, this record will include the:

- the facts and cause;
- any effects identified;
- the action(s) that have been taken to contain the data breach and ensure there is no recurrence (such as establishing more robust processes or providing further training for individuals).

14. The DPO will meet with the Head-Teacher as soon as practicable after the event to review the circumstances of the data breach and consider the actions that are needed to prevent a recurrence. They will also consider what actions could be reasonably be taken to recover or retrieve lost or stolen personal data, using expert external assistance if necessary.