Willow Bank Junior School

Data Protection Policy

Statutory policy

Version	***Last Review***	***Next Review***	***Committee***	***Comments***
1.0	May 2018	May 2020	FGB	
1.0	September 2020	September 2022	FGB	No changes
2.0	March 2023	March 2025	FGB	

Introduction

Willow Bank Junior School is committed to the protection of all personal and sensitive data for which it holds responsibility as the Data Controller. This policy applies to all school data, regardless of whether it is in paper or electronic format and where it is stored.

This policy meets the requirements of the Data Protection Act 2018 (which incorporates the General Data Protection Regulation) and is based on guidance published by the Information Commissioner's Office (ICO) and the Department for Education (DfE).

The school is also committed to ensuring that its staff and governors are aware of data protection policies and legal requirements, and adequate training is provided to them. All staff and governors should note that the Act makes provision for significant fines to be levied in the event of non-compliance.

The requirements of this policy are mandatory for all staff employed by the school and any third party contracted to provide services within the school.

Principles

The Data Protection Act 2018 sets out six data protection principles that the school must follow when processing data. Data must be:

- Processed fairly, lawfully and in a transparent manner
- Used for specified, explicit and legitimate purposes
- Used in a way that is adequate, relevant and limited
- Accurate and kept up-to-date
- Kept no longer than is necessary
- Process the data in accordance with the data subject's rights
- Processed in a manner that ensures appropriate security of the data

Categories of Data

The Data Protection Act 2018 refers to **Personal data** and **Special categories of personal data**.

Personal data means any information relating to an identifiable person who can be directly or indirectly identified in particular by reference to an identifier.

Sensitive categories of personal data (previously known as 'sensitive personal data') includes race, ethnic origin, politics, religion, trade union membership, biometrics, health and sexual orientation.

Note that the DfE consider it best practice that data such as free school meal status, pupil premium eligibility, elements of special educational need information, some behaviour data and Children's Services interactions are also treated with the same care as the special categories set out in law.

Roles and Responsibilities

The Data Controller

- Our school processes personal information relating to pupils, staff and visitors (defined as 'Data Subjects') and is therefore a Data Controller.
- The governing body has overall responsibility for ensuring that the school complies with its obligations under the Data Protection Act 2018.
- The Headteacher will ensure the provisions of this policy are in place and that all staff are aware of their data protection obligations.
- Day to day responsibility for data protection will reside with the Data Protection Offier (DPO).
- The school is registered as a Data Controller with the ICO and renews this registration annually.

Data Protection Officer

The Data Protection Officer will:

- Act as the contact point for all data protection issues and queries from data subjects and the ICO (e.g. for Subject Access Requests, data breaches) following the agreed procedures (see appendices).
- Maintain appropriate documentation relating to data processing.
- Undertake the training necessary to fulfil their role and ensure staff have access to appropriate training and updates.
- Monitor compliance with all aspects of data protection.
- Provide advice relating to Data Protection Impact Assessments (DPIA) (e.g. before introducing a new data processing system).

School Staff

- All school staff, in whatever role, have a duty to comply with this policy. Failure to comply may result in disciplinary action.
- Staff must report any data related concerns or breaches immediately to the DPO.

Data Processors

- The school uses a range of third parties to process data on our behalf, e.g. payroll, catering, communications. The school will ensure that all data processors are compliant with the Data Protection Act 2018.

Sharing Data

- Where data is routinely shared with other organisations (e.g. Local Authority, DfE, NHS) the school will ensure this is made clear in the Privacy Notice and that appropriate protocols are in place.

Data Protection Documentation

Privacy Notices

The school will make available Privacy Notices for Pupils/Parents, Staff and Governors that set out how the school will make use of their personal data. These will be made available via the school website.

Consent

Where required the school will seek and record specific consent from data subjects (e.g. image permissions, email marketing).

Data Protection Audit, Record Keeping and Logs

The school will maintain suitable records which detail all data that is collected, processed and where appropriate shared. The London Grid for Learning (LGfL) audit tool will be used for this purpose. In addition the school will keep records for other key areas including:

- Subject Access Requests
- Data Breaches
- Data Retention Schedule
- Data Disposal/Destruction Log
- Data Protection Impact Assessments
- Requests for changes to data
- A general description of the technical and organisational security measures that are in place.

Subject Access Requests

Under the Data Protection Act, pupils (or their parents for children under 13) have a right to request access to information the school holds about them. This is known as a Subject Access Request (SAR).

The SAR process and timescales are provided in Appendix 2.

In addition, maintained schools should be aware of Regulation 5 of the Education (Pupil Information) (England) Regulations 2005 that gives parents the right of access to their child's educational record, free of charge, within 15 school days of a request.

Freedom of Information Act

The school will comply with the Freedom of Information Act 2000 (FOI). All FOI requests will be directed to the DPO who will follow the procedures outlined in Appendix 3.

The school will comply with the requirement to produce a publication scheme, following the guidance available from the ICO.

Security and Storage

The school will ensure that appropriate technical and organisational measures are in place to protect school data, and to ensure that staff and governors are only able to access data that is relevant to their role.

Sensitive or personal information and data should not be removed from the school site, however the school acknowledges that some staff may need to transport data between the school and their home in order to access it for work in the evenings and at weekends. This may also apply in cases where staff have offsite meetings or are on school trips with pupils.

Guidelines for staff, in order to reduce the risk of personal and sensitive data being compromised, are provided in Appendix 4.

Retention and Disposal

The school recognises that the secure disposal of redundant data is an integral element to compliance with legal requirements and an area of increased risk.

All data shall be destroyed or eradicated to agreed levels, meeting recognised national standards. All data held in any form of media (paper, electronic) shall only be passed to a disposal partner with demonstrable competence in providing secure disposal services. A destruction record will be held for all data and devices that are disposed of.

Timescales for retaining data will be in accordance with the guidelines provided by the Information and Records Management Society (www.irms.org.uk) in their Information Management Toolkit for Schools.

Training

All staff and governors will be provided with data protection training as part of their induction process.

Data protection training, briefings and updates will also be provided for all staff and governors as required, but at least every two years.

Appendix 1 – Data Breach Information and Procedures

Data protection breaches can be caused by a number of factors such as:

- Loss or theft of pupil, staff or governing body data and/or equipment or paperwork on which data is stored
- Inappropriate access controls allowing unauthorised use
- Poor data destruction procedures
- Human error such as sending an email to the wrong person
- Cyber-attack, hacking or ransomeware

In the event of a breach, the procedures below should be followed:

1. Any data protection incident should be reported immediately to the school's DPO and Headteacher.
2. If required, appropriate actions should be taken to halt the breach, and/or prevent further breaches.
3. The DPO must report any significant data protection incidents to the ICO. This should take place within **72 hours** of the breach being detected, where feasible. If in doubt as to the significance of the incident, seek external advice which could involve contacting the ICO. If some details of the breach are yet to be determined, it would be appropriate to make an initial report to the ICO, followed up by a further report once more is known.
4. The Chair of Governors should be informed as soon as possible. Other agencies, as appropriate, may need to be informed depending on the breach, e.g. police, Action Fraud, social services.
5. Where the breach involves the disclosure of the personal data of specific individuals, they should usually be notified.
6. Fully investigate the breach and review all related policies and procedures to make any necessary changes.
7. Provide additional training to staff as appropriate.
8. Review whether any disciplinary action should be taken.
9. If the nature of the breach could result in adverse publicity, the school may want to prepare a statement for publication.
10. A full record should be kept of all data breaches, including all the steps taken, whether reportable or not.

Additional Notes

In the event of a data breach, the following areas will need to be considered:

- The type of data and its sensitivity
- What protections were in place (e.g. encryption)
- What has happened to the data
- Whether the data could be put to any illegal or inappropriate use
- How many people are affected
- What type of people have been affected (pupils, staff etc) and whether there are wider consequences to the breach.

Appendix 2 – Subject Access Request Process and Timescales

A Subject Access Request (SAR) is a request for personal data about the applicant. Where pupils are under the age of 13, a SAR will be made on their behalf by the parent or guardian.

All SARs must be in writing, either paper or electronic, and should be directed to the DPO who will follow the procedure outlined below:

1. Clarify that this is a SAR and not some other request for information (i.e. a FOI or 'educational record' request).
2. Confirm the identity of the person making the request.
3. If it is unclear what information is being requested, ask for further details from the applicant.
4. Check that the information is available.
    a. If the information is not available, inform the applicant.
    b. If the information is available, note the date that the SAR was received or, in the case of further details being requested, the date that those were received. The school now has **one calendar month** to respond.
5. Check whether the information requested contains information about any third-party. If it does then undertake one or more of the following steps:
    a. Seek permission to disclose the information from the third-party concerned.
    b. Redact/summarise the information to protect the identity of the third-party.
    c. Withhold the information to protect the rights of the third-party.
6. Ensure that the information to be supplied is clear and understandable, e.g. any complex codes or terms are explained.
7. Supply the information requested in an appropriate format. E.g. if the request is made electronically, the information should be provided in an electronic format.
8. Keep a record of the SAR and any information that was supplied.

Additional Notes

- The school must provide a copy of the information free of charge. However, the school can charge a 'reasonable fee' when a request is manifestly unfounded or excessive, particularly if it is repetitive. The school may also charge a reasonable fee to comply with requests for further copies of the same information. The fee must be based on the administrative cost of providing the information.
- The school will be able to extend the one month period of compliance by a further two months where requests are complex or numerous. If this is the case, the school must inform the applicant within one month of the receipt of the request and explain why the extension is necessary.
- The school might also decide to withhold some information. Examples of some information which (depending on the circumstances) it might be appropriate to withhold include:
    - Information that might cause serious harm to the physical or mental health of the pupil 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
- More information about SARs is available on the ICO website.

Appendix 3 – Freedom of Information Process and Timescales

The school has a publication scheme, which outlines the information that is routinely made available. This can be found on the school website.

A Freedom of Information (FOI) request may be made by any member of the general public, as they have a right to know about the activities of public authorities, which includes schools. The school will normally disclose the information requested in whole or part unless there is a clear and accepted reason not to do so.

All FOI requests must be in writing, either paper or electronic, and must contain the applicant's contact details. All requests should be directed to the DPO who will follow the procedure outlined below:

1. Clarify that this is a FOI request and not some other request for information (i.e. a SAR or an 'educational record' request).
2. If it is unclear what information is being requested, ask for further details from the applicant.
3. Check that the information is available:
    a. If the information is not available, inform the applicant.
    b. If the information is available, note the date the FOI request was received or, in the case of further details being requested, the date that those were received. The school now has **20 days** to respond.
4. Check whether there is any good reason for refusing to disclose part or all of the information requested. See guidance from the ICO if in any doubt.
5. Ensure that the information to be supplied is clear and understandable.
6. Supply the information requested in an appropriate format. E.g. if the request is made electronically, the information should be provided in an electronic format.
7. Keep a record of the FOI request and any information that was supplied.

Additional Notes

- The school may charge for the cost of copying and postage, where appropriate.
- The school may refuse an entire request under various circumstances, e.g.
    - It would cost too much or take too much staff time to deal with the request (although note that the ICO guidance relating to this aspect indicates that the work required would have to be very substantial before a refusal would be acceptable).
    - Where complying might prejudice someone's commercial interests. However, it has to pass the 'Public Interest Test', i.e. that on balance the public interest in withholding the information outweighs the public interest in disclosing it.
    - The request is vexatious.
    - The request repeats a previous request from the same person.
- Further advice on when a FOI request may be refused is available from the ICO.

Appendix 4 – Staff Guidelines to Protect Data

The following guidelines are in place for staff in order to reduce the risk of personal and sensitive data being compromised:

- Paper copies of data or personal information should be stored out of sight in locked cupboards and filing cabinets.
- Paper copies of data or personal information should not be taken off the school site. If these are misplaced they are easily accessed. If there is no way to avoid taking a paper copy of data off the school site, the information should not be on view in public places or left unattended under any circumstances.
- Unwanted paper copies of data, sensitive information or pupil files should be shredded. This also applies to handwritten notes if the notes reference any other staff member or pupil by name.
- Care must be taken to ensure that printouts of any personal or sensitive information are not left in printer trays or photocopiers.
- If information is being viewed on a computer, staff must ensure that the window and documents are properly shut down before leaving the computer unattended. Sensitive information should not be viewed on public computers.
- If it is necessary to transport data away from the school, it should be downloaded onto an **encrypted** USB stick provided by the school. The data should not be transferred onto any home or public computers. Work should be edited from the USB and saved onto the USB only.