# Wilson's School

# Data Protection Policy

**Date approved by Trust Board: Spring 2026**

**Date of next review: Spring 2028**

**DATA PROTECTION POLICY**

## 1. Aims

Wilson's School aims to ensure that all personal data collected about staff, pupils, parents, trustees, visitors and other individuals is collected, stored and processed in accordance with UK data protection law. This policy applies to all personal data, regardless of whether it is in paper or electronic format.

## 2. Legislation and guidance

This policy meets the requirements of the:

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

It is based on guidance published by the Information Commissioner's Office (ICO) on UK GDPR for organisations. It meets the requirements of the Protection of Freedoms Act 2012 when referring to the use of biometric data. It also reflects the ICO's code of practice for the use of surveillance cameras and personal information.

## 3. Definitions

| Term | Definition |
|---|---|
| Personal data | Any information relating to an identified, or identifiable, individual.<br>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.<br>It includes information that would identify an individual to the person to whom it is disclosed because of any special knowledge that they have or can obtain. |
| Special categories of personal data | Personal data which is more sensitive and so needs more protection, including information about an individual's:<br>• Racial or ethnic origin<br>• Political opinions<br>• Religious or philosophical beliefs<br>• Trade union membership<br>• Physical or mental health<br>• An individual's sex life or sexual orientation<br>• Genetic or biometric data for the purpose of uniquely identifying a natural person |

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

## 4. The data controller

Wilson's School processes personal data relating to parents, guardians, carers, pupils, staff, trustees, alumni, members, trustees, visitors and others, and therefore is a data controller. The school is registered as a data controller with the ICO and will renew this registration annually or as otherwise legally required.

## 5. Roles and responsibilities

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

5.1 **Trust Board** – the Trust Board has overall responsibility for ensuring that the school complies with relevant data protection obligations.

5.2 **Data Protection Officer** - The data protection officer (DPO) is responsible for overseeing the implementation of this policy, monitoring compliance with data protection law, and developing related policies and guidelines where applicable. They will provide an annual report of their activities to the Trust Board and, where relevant, report to the board their advice and recommendations on school data protection issues. The DPO is also the first point of contact for individuals whose data the school processes, and for the ICO. The DPO for Wilson's School is contactable in the following ways:
E-mail: dpo@wilsonsschool.sutton.sch.uk
Telephone: 0208 773 2931
Post: Wilson's School, Mollison Drive, Wallington, SM6 9JW.

5.3 **Executive Head**– the Executive Head acts as the representative of the data controller on a day-to-day basis.

5.4 **All staff** - Staff are responsible for:

- Processing and storing any personal data in accordance with this policy;

- informing the school of any changes to their personal data, such as a change of address;
- contacting the DPO in the following circumstances:
  - with any questions about the operation of this policy, data protection law, retaining personal data or keeping personal data secure;
  - if they have any concerns that this policy is not being followed;
  - if they are unsure whether or not they have a lawful basis to use personal data in a particular way;
  - if they need to rely on or record consent, draft a privacy notice, deal with an individual's request to invoke their data protection rights, or transfer personal data outside the UK;
  - if there has been a data breach;
  - whenever they are engaging in a new activity that may affect the privacy rights of individuals;
  - if they need help with any contracts or sharing personal data with third parties.

## 6. Data Protection Principles

The UK GDPR is based on data protection principles that 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 fulfil the purposes for which it is processed;
- accurate and, where necessary, kept up to date;
- kept for no longer than is necessary for the purposes for which it is processed;
- processed in a way that ensures it is appropriately secure.

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

## 7. Collecting Personal Data

### 7.1 Lawfulness, fairness and transparency

Wilson's School will only process personal data where one of 6 'lawful bases' (legal reasons) to do so under data protection law has been identified.

- The data needs to be processed so that the school can **fulfil a contract** with the individual, or the individual has asked the school to take specific steps before entering into a contract.
- The data needs to be processed so that the school can **comply with a legal obligation.**
- The data needs to be processed to ensure the **vital interests** of the individual e.g., to protect someone's life.
- The data needs to be processed so that the school, as a public authority, can **perform a task in the public interest, or exercise its official authority.**

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

### 7.2 Special Category Data

For special categories of personal data, the school will also meet one of the special category conditions for processing under data protection law as set out in Chapter 2, sections 8 & 10 of the Data Protection Act 2018. Information relating to criminal convictions shall only be held and processed where there is legal authority to do so.

### 7.3 Limitation, Minimisation and Accuracy

Wilson's School will only collect personal data for specified, explicit and legitimate reasons. The reasons will be explained to the individuals when first collecting their data. This will be through the relevant privacy notice, and any updated privacy notice from time to time.

If the school wants to use personal data for reasons other than those given when it was first obtained, or as stated in privacy notices, or where there would be no expectation that an individual's data would be used for such a purpose, the individuals concerned will be informed in advance, and consent sought where necessary.

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

The School's aim is to keep data accurate and, where necessary, up to date. Inaccurate data will be rectified or erased when appropriate. When staff no longer need the personal data they hold, they must ensure it is deleted, destroyed or anonymised.

## 8. Sharing and Using Personal Data

Full details of the ways in which the School will process, use and share the personal data of data subjects can be found in the relevant Privacy Notice.

The School will not normally share personal data with third parties , but the following provides a non-exhaustive list of the most usual reasons for disclosure of personal data to a third party:-

- To give a confidential reference relating to a current or former employee, volunteer or pupil.
- There is an issue with a pupil or parent/carer that puts the safety of staff at risk.
- For reasons relating to safeguarding / child protection.
- It is necessary to liaise with other agencies and, if appropriate, consent will be sought as necessary before doing this.
- To disclose details of a pupil's medical or health condition where it is in the pupil's interests to do so, for example for medical advice, insurance purposes or to organisers of a school visit.

- To provide information to another educational establishment to which a pupil is transferring.
- For the purpose of obtaining legal advice.
- Suppliers or contractors need data to enable the school to provide services and to meet its duties to staff and pupils – for example, IT companies. When doing this, the school 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 shared;
    - 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.
- There is a legal requirement to do so, for example law enforcement and government bodies, 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 safeguarding obligations;
    - research and statistical purposes, as long as personal data is sufficiently anonymised or consent has been provided.

The school may also share personal data with emergency services, local authorities and other appropriate agencies to help them to respond to an emergency situation that affects any of the school's pupils or staff.

Where a pupil seeks to raise issues confidentially with a member of staff and expressly withholds their agreement to their personal data being disclosed to their parents/guardians, the school will maintain confidentiality unless it has reasonable grounds to believe that the pupil does not fully understand the consequences of withholding their consent, or where the School believes disclosure will be in the best interests of the pupil or other pupils. Such maters will be dealt with in accordance with the Safeguarding and Child Protection Policy. Guidance is also available here: Information sharing advice for safeguarding practitioners - GOV.UK

The school may make use of information (or may transfer information to any association, society or club) for the purpose of maintaining contact with pupils or ex pupils and their parents/guardians or for fundraising, marketing or promotional purposes and to maintain relationships with pupils and their parents/guardians whilst they are at the school and once they have left.

The school may make personal data, including special category data available to staff for the planning of school visits, curricular or extra-curricular activities and the school may use photographs and moving images of pupils in accordance with internal procedures.

If the school were to transfer personal data to a country or territory outside the European Economic Area, it will take steps required to do so in accordance with data protection law.

## 9. Subject Access Requests and Other Rights of Individuals

### 9.1 Subject Access Requests

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

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

Subject access requests must be submitted in writing, either by letter or email to the DPO. They should include the name of the individual making the request, their correspondence address, their contact number and email address as well as details of the information requested.

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

### 9.2 Children and subject access requests

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

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

### 9.3 Responding to subject access requests

When responding to requests, the school:

- may ask the individual to provide 2 forms of identification;
- may contact the individual via telephone to confirm the request was genuinely made;
- will respond without delay and within 1 month of receipt of the request, unless the request falls during the school holidays, in which case the school will deal with the request, within 1 month of the return to school. The individual will be informed of this within 1 month, with an explanation as to why the extension is necessary;
- may tell the individual that a response will be provided within 3 months of receipt of the request, where a request is complex or multifaceted. The individual will be informed of this within 1 month, with an explanation as to why the extension is necessary;
- will provide the information free of charge.

Information may not be disclosed 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;
- would include another person's personal data that can't reasonably be anonymised, and the other person's consent has not been obtained and it would be unreasonable to proceed without it;
- is part of certain sensitive documents, such as those related to crime, immigration, legal proceedings or legal professional privilege, management forecasts, negotiations, confidential references, or exam scripts.

If the request is unfounded or excessive, the school may refuse to act on it, or charge a reasonable fee which takes into account administrative costs. The school will consider whether the request is repetitive in nature when making this decision. The school will take into account relevant guidance from the ICO when reaching a decision.

When a request is refused, an explanation will be provided to the individual, and the requester will be provided with information about their right to complain to the ICO, or they can seek to enforce their subject access right through the courts.

**9.4 Other data protection rights of the individual**

In addition to the data protection rights detailed above, individuals also have the right to:

- withdraw their consent to processing at any time;
- ask the school 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;
- object to processing which has been justified on the basis of public interest, official authority or legitimate interests;
- challenge decisions based solely on automated decision making or profiling (decisions taken with no human involvement, that might negatively affect them);

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

**10. Biometric Recognition Systems**

*Note that in the context of the Protection of Freedoms Act 2012, a "child" means a person under the age of 18.*

Where the school use pupils' biometric data as part of an automated biometric recognition system (for example, use of fingerprints or facial recognition for registration), it will comply with 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 before it takes any biometric data from their child and first process it.

Parents/carers and pupils have the right to choose not to use the school's biometric system(s). The school will provide alternative means of accessing the relevant services for those pupils.

Parents/carers and pupils can object to participation in the school's biometric recognition system(s), or withdraw consent, at any time, and the school will make sure that any relevant data already captured is deleted.

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

**11. CCTV**

Wilson's School uses CCTV in various locations around the school site to ensure it remains safe. The school adheres to the ICO's code of practice for the use of CCTV. The school does not need to ask individuals' permission to use CCTV, but it is made clear to individuals by way of signage where they are being recorded. Security cameras are clearly visible. Any enquiries about the CCTV system should be directed to the DPO.

**12. Photographs and videos**

As part of school activities, photographs and recorded images of individuals within the school may be taken.

On joining the school written consent is obtained from parents/carers and/or pupils, for photographs and videos to be taken of pupils for use within school for displays and for communication, marketing and promotional materials and online content. The School

expects parents and pupils to feel able to support the School in using pupil images to celebrate achievements, promote the work of the School and for important administrative purposes such as identification and security. As detailed in paragraph 9.2 above where a child is capable of understanding their rights and making decisions in relation to their personal data it is they, as the data subject, that can give consent (not their parent/carer). The school will, however, take into account the wishes of parents/carers where reasonably possible.

When using photographs and videos of pupils they will not be accompanied with any other personal information about the child, to ensure they cannot be identified outside the school community, although the child's first name and year group and or House may be used on the school's website. When we are aware that pupils images are likely to be used in the media, we make efforts to ensure that pupils and parents are informed that this is the case. Consent can be refused or withdrawn at any time. If consent is withdrawn, the photograph or video will be deleted and not distributed further.

Any photographs and videos taken by parents/carers at school events of their own children for their own personal use are not covered by data protection legislation.

Certain images are necessary for the ordinary running of the School and its community. The school is entitled lawfully to process such images and take decisions about how to use them subject to any reasonable objection raised.

**13. Artificial Intelligence (AI)**

The school may make limited use of Artificial Intelligence (AI) to support educational, administrative, and operational activities. When using AI tools members of staff are not permitted to enter personal and sensitive data into unauthorised generative AI tools or chatbots. If personal and/or sensitive data is entered into an unauthorised AI tool it must be treated as a data breach. The school will not use AI to make solely automated decisions that have legal or similarly significant effects on pupils, parents, or staff. Staff have been provided with guidance on the appropriate and safe use of AI tools. The school will regularly review its use of AI to ensure ongoing compliance with data protection requirements and best practice.

**14. Data protection by design and default**

The school will put measures to integrate data protection into all data processing activities, including:

- appointing a suitably qualified DPO, and ensuring they have the necessary resources to fulfil their duties and maintain their expert knowledge;
- only processing personal data that is necessary for each specific purpose of processing, and always in line with the data protection principles set out in relevant data protection law;

- completing data protection impact assessments where the school's processing of personal data presents a high risk to rights and freedoms of individuals, and when introducing new technologies (the DPO can advise on this process);
- integrating data protection into internal documents including this policy, any related policies and privacy notices;
- regularly training members of staff on data protection law, this policy, any related policies and any other data protection matters;
- regularly conducting reviews of privacy measures and addressing areas for further development;
- putting appropriate safeguards in place if any personal data is to be transferred outside of the UK, where different data protection laws may apply.

**15. Data security and storage of records**

The school will take reasonable steps to 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, staff are given the following guidelines and are reminded at regular intervals:

- Paper-based records and portable electronic devices, such as laptops, iPads and hard drives that contain personal data are stored carefully when not in use.
- Papers containing confidential personal data should not be left on office and classroom desks, on staffroom tables, pinned to notice/display boards, on printers or photocopiers or left anywhere else where there is general access.
- Where paper-based personal information needs to be taken off site, staff must take appropriate precautions to protect the data.
- Where staff are working off-site and are accessing personal data via a computer or lap top or iPad appropriate precautions are taken to ensure no unauthorised access to the data is possible.
- Passwords that are at least 8 characters long containing letters and numbers are used to access school computers, laptops and other electronic devices. Staff and pupils are forced to change their passwords at regular intervals.
- Use of USB devices is discouraged but in the unlikely event of them being used they should be password protected.
- Personal devices used to access school data must follow the same security measures, including strong passwords and encryption.
- Two factor authentication (2FA) should be used for accessing sensitive systems and data.
- Where there is a need to share personal data with a third party, reasonable steps should be taken to ensure it is stored and transferred securely and adequately protected.

**16. Disposal of records**

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

For example, the school will shred or incinerate paper-based records, and overwrite or delete electronic files. The school may also use a third party to safely dispose of records on the school's behalf. In this case the third party is required to provide sufficient guarantees that it complies with data protection law.

Staff records will be retained for 7 years after leaving (aside keeping a very minimal amount of information to allow the school to validate that a former staff member was an employee) unless there are ongoing allegations in relation to the sexual abuse of pupils. Student records will be deleted 7 years after students have left the school, aside keeping a very minimal amount of information to allow the school to validate that a former student was on roll. For other records the school has regard to the IRMS document retention toolkit for academy schools.

**17. Training**

Staff are provided with data protection training as part of their induction process. Data protection also forms part of continuing professional development for members of staff; the frequency of training and what is covered is differentiated for members of staff with different roles.

**18. Personal data breaches**

In the event of a suspected data breach, the procedure set out in appendix 1 will be followed.

*Linked policies:*
Acceptable Use Policy
Child Protection and Safeguarding Policy
IT Security Policy
Privacy Notices
Freedom of Information Policy and publication scheme

Appendix 1

**DATA BREACH PROCEDURE**

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

1. On finding or causing a breach, or potential breach, the staff member or data processor must immediately notify the DPO, or in their absence a member of the Senior Leadership Team.
2. The DPO/SLT member will investigate the report and determine whether a breach has occurred. To decide, the factors to be considered are whether personal data has been accidentally or unlawfully:
    a. Lost
    b. Stolen
    c. Destroyed
    d. Altered
    e. Disclosed or made available where it should not have been
    f. Made available to unauthorised people
3. Staff and trustees must cooperate with the investigation (including allowing access to information and responding to questions).
4. If a breach has occurred or it is considered to be likely that is the case, the DPO/SLT member will alert relevant staff members. If necessary, the SLT member will make sure that the DPO is notified of the breach (or potential breach).
5. The DPO/SLT member, when dealing with or responding to a breach (or potential breach) will make all reasonable efforts to contain and minimise the impact of the breach, assisted by relevant staff members or data processors where necessary, and take external advice when required (e.g. from IT providers).
6. An assessment will be made of the potential consequences, based on how serious they are, and how likely they are to happen, before and after the implementation of steps to mitigate the consequences.
7. An assessment will be made as to whether the breach must be reported to the ICO and the individuals affected using the ICO's self-assessment tool. Where the ICO must be notified, the DPO will do this via the 'report a breach' page of the ICO website, or through its breach report line (0303 123 1113), within 72 hours of the school's awareness of the breach.
8. As required, the report will set out a description of the nature of the personal data breach including, where possible:
    a. The categories and approximate number of individuals concerned.
    b. The categories and approximate number of personal data records concerned.
    c. The name and contact details of the DPO.
    d. A description of the likely consequences of the personal data breach.
    e. A description of the measures that have been, or will be taken, to deal with the breach and mitigate any possible adverse effects on the individual(s) concerned.

If all the above details are not yet known, the school will report as much as possible within 72 hours of the school's awareness of the breach. The report will explain that there is a delay, the reasons why, and when it is expected to have further information. The remaining information will be submitted as soon as possible.

9. Where appropriate, the school will communicate with individuals whose personal data has been breached.
10. An assessment will also be made, in light of the investigation and any engagement with affected individuals, whether to notify any relevant third parties who can help mitigate the loss to individuals – for example, the police, insurers, banks or credit card companies.
11. The DPO will document each breach, irrespective of whether it is reported to the ICO. For each breach, this record will include the:
    a. Facts and cause
    b. Effects
    c. Action taken to contain it and ensure it does not happen again (such as establishing more robust processes or providing further training for individuals)

    Records of all breaches will be on the school's computer system.
12. The DPO will meet with the SLT (a) following a reportable breach to review what happened and how it can be stopped from happening again. This meeting will happen as soon as reasonably possible; and (b) at least annually to assess recorded data breaches and to identify any trends or patterns requiring action by the school to reduce risks of future breaches.