THE STONEHENGE

SCHOOL

# DATA PROTECTION POLICY

2026

| | |
|---|---|
| Statutory | Yes (Recommended) |
| 3rd Party Model | One West |
| Review Frequency | Annual |
| Review | One West DPO Service |
| Approving Authority | Headteacher |
| Published on School Website | Yes |

| **Action** | **Date** | **Comment** |
|---|---|---|
| Last Approved | Jan 2026 | |
| Due Review | Dec 2026 | |

# Data Protection Policy

## Contents


1. Aims ..... 2
2. Scope ..... 2
3. Distribution ..... 2
4. Definitions ..... 2
5. Roles and Responsibilities ..... 4
6. Data Protection Officer (DPO) ..... 5
7. Data Subject Rights ..... 5
8. Data Protection Principles ..... 7
9. Processing Personal Data ..... 9
10. Third Parties with Access to Personal Data ..... 11
10.1. Data Sharing ..... 11
10.2. Third-Party Processors ..... 11
11. Data Protection by Design and Default ..... 12
12. Personal data breaches or near misses ..... 12
13. Biometric Recognition Systems ..... 12
14. Destruction of records ..... 13
15. Training ..... 14
16. Monitoring Arrangements ..... 14
17. Complaints ..... 14
18. Legislation and Guidance ..... 15
19. Links with Other Policies ..... 15
20. Approval ..... 15

Appendix 1 – Examples of Special Category Data that we process ..... 16

Appendix 2 – Subject Access Request Procedure (SAR) ..... 17


| Version | Date | Summary of changes | Author |
|---|---|---|---|
| V1.0 | June 2019 | Initial | One West |
| V2.0 | Aug 2023 | Incorporated Special Category Data Policy. Removal of reference to age in consent. | One West |
| V2.1 | Aug 2025 | Addition of right to complain, in accordance with DUAA, as well as a reference to AI tools under Automated Decision Making. Addition of reference to recognised legitimate interests. | One West |

# Data Protection Policy

## 1. Aims

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

The Stonehenge School are registered as a data controller with the Information Commissioner.

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

## 2. Scope

This policy applies to anyone who has access to data and/or is a user of The Stonehenge School's ICT systems, both in and out of The Stonehenge School, including staff, volunteers, visitors, contractors, and other community users.

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

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

## 3. Distribution

This policy is available on the The Stonehenge School's website and in hard copy from the The Stonehenge School office.

## 4. Definitions

**Personal data** - Any combination of data items which could identify a living person and provide specific information about them, their families or circumstances. The term covers both facts and opinions about an individual. We may process a wide range of personal data of staff (including volunteers) as part of our operation. A non-exhaustive list of examples of the types of personal data that we process may be found in our privacy notices.

**Special category personal data** - Formerly known as "sensitive personal data", special category data is information that is a lot more sensitive to that person and needs more protection. These are:

- racial or ethnic origin
- political opinions
- religious / philosophical beliefs
- trade union membership
- genetic data
- biometric data (for identification purposes)
- health data (mental and physical)
- sex life or sexual orientation

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

**Data Subject(s)** - The data subject is the person about whom the personal data relates or identifies.

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

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

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

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

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

Note, we do NOT *share* data with our data processors, as these are processing it under our data controllership.

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

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

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

## 5. Roles and Responsibilities

**Governing Body** - Have overall responsibility for ensuring that The Stonehenge School complies with all relevant data protection obligations.
**Data Protection Lead** - acts with the delegated authority of the Governors on a day-to-day basis and will liaise with the DPO. In their absence, in case of emergency, this role will be delegated to The Headteacher.

**All other staff (as defined in scope)** - All staff are responsible for:

- Familiarising themselves with and complying with this and related policies. The learning culture within the organisation seeks the avoidance of blame and is key to allowing individuals the confidence to report genuine mistakes. However, staff should be aware, that a deliberate or reckless disregard of this policy could result in disciplinary action being taken;
- Taking care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse at all times. All staff should adopt the approach that they should treat the personal data of others with the same care with which they would treat their own;
- Only using computers and other devices authorised by The Stonehenge School for accessing and processing personal data ensuring that they are properly "logged-off" at the end of any session in which they are using personal data; and locking devices when they are temporarily left unattended at any point (Windows Button □ + L is a handy shortcut);
- Storing, transporting and transferring data using encryption and secure password protected devices;
- Not transferring personal data offsite or to personal devices
- Deleting any data they hold in line with this policy, the Records Management Policy, and the retention schedule;
- Informing The Stonehenge School of any changes to their personal data, such as a change of address;
- Reporting to the Data Protection Lead, or in their absence the DPO in the following circumstances:
    - Any questions about the operation of this policy, data protection law, retaining or sharing personal data or keeping personal data secure;
    - If they have any concerns that this policy is not being followed;
    - If they are unsure whether they have a lawful basis upon which to use personal data in a particular way;
    - If they need to rely on or capture consent, deal with data protection rights invoked by an individual, or transfer personal data outside the UK and European Economic Area;
    - The discovery of a data breach or near miss (immediate action is required) – please refer to the Data Breach Policy and section 12 of this policy;
    - Whenever they are engaging in a new activity that may affect the privacy rights of individuals;

- If they are to share personal data with a data processor, for example a contractor or someone offering a service, in which case a contract is likely to be required and potentially a data protection impact assessment (DPIA), please see - *Sharing Personal Data* (section 10).

## 6. Data Protection Officer (DPO)

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

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

One West (Bath and North-East Somerset Council)
Guildhall, High Street, Bath, BA1 5AW

Email: i-west@bathnes.gov.uk
Telephone: 01225 395959

Under usual circumstances the Data Protection Lead will be the point of contact with the DPO.

## 7. Data Subject Rights

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

### 7.1. Right to be informed.

We advise individuals how we will use their data through the use of transparent privacy notices and other documentation, such as data capture and consent forms where appropriate.

### 7.2. Right of access

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

- Confirmation that their data is being processed;
- Access to their personal data;
- Other supplementary information – this largely corresponds to the information that should be provided in a privacy notice.

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

### 7.3. Right to rectification

Individuals have the right to ask us to correct information they think is inaccurate or incomplete. We have a duty to investigate any such claims and rectify the information where appropriate within one calendar month, unless an extension of up to a further two calendar months can be justified.

### 7.4. Right to erasure

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

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

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

### 7.5. Right to restrict processing

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

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

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

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

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

### 7.6. Right to data portability

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

### 7.7. Right to object

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

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

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

### 7.8. Right to complain

Individuals have the right to complain about the way in which an organisation processes their personal data. This is the first stage, before the Information Commissioner will consider a personal data complaint. Please see our Complaints Policy for further information.

## 8. Data Protection Principles

Data protection legislation is based on seven key data protection principles that The Stonehenge School complies with.

The principles say that personal data must be:

- **Processed lawfully, fairly and in a transparent manner** – we will explain to individuals why we need their data and why we are processing it – for example on consent forms (where consent is used as the basis for processing), and in our Privacy Notice(s). We review our documentation and the basis for processing data on a regular basis.
- **Collected for specified, explicit and legitimate purposes** – we explain these reasons to the individuals concerned when we first collect their data. If we wish to use personal data for reasons other than those given when the data was first obtained, we will inform the individuals concerned before doing so, and will seek consent where necessary and appropriate unless the new purpose is compatible with that in respect of which consent was given, or there is another lawful basis for sharing the information. In which case, we will document the basis for processing.
- **Adequate, relevant and limited to what is necessary to fulfil the purposes for which it is processed -** we must only process the minimum amount of personal data that is necessary in order to undertake our work.
- **Accurate and, where necessary, kept up to date** – we will check the details of individuals on our databases at appropriate intervals and maintain the databases. We will consider and respond to requests for inaccurate data to be rectified in accordance with the Data Protection Act 2018.
- **Kept for no longer than is necessary for the purposes for which it is processed** – we review what data we hold at appropriate intervals – for example upon the annual review of the Record of Processing Activities (or sooner if needed). When we no longer need the personal data we hold, we will ensure that it is deleted or anonymised in accordance with the retention schedule. We only keep personal data, including special category data, in an identifiable form for as long as is necessary for the purposes for which it was collected, or where there is a legal obligation to do so;
    - We have a retention and disposal/records management policy which governs how long all data including special category data shall be retained for. This policy is complied with and reviewed regularly;

- Once the data is no longer needed, we delete it, securely destroy it in line with our retention and disposal policy, or render it permanently anonymous.

- **Processed in a way that ensures it is appropriately secure** – The Stonehenge School implements appropriate technical measures to ensure the security of data and systems for staff and all users. Please refer to the Information Security Policy
  - We adopt a risk- based approach to taking data offsite. Unless absolutely necessary, hard copies of special category personal data will not be removed from our premises.
  - Any decision to remove the information must be based on the business need of the organisation or in the best interests of the individual, rather than for the convenience of the individual member of staff. It is always preferable for any special category data to be accessed via appropriately encrypted means rather than hard copy, when off-site.
  - If there is no reasonable alternative to removing hard copies from The Stonehenge School's site, the following procedure will apply:
    i. A record of what information has been removed will be logged on site with the office so that there is a record of what has been removed – for example health data in trip packs;
    ii. We adopt a risk-based approach, for example hard copy personal data with lower sensitivity (e.g. notebooks) may be taken off site, but if left in a vehicle must be locked in the boot, never left in a visible place, only for the shortest period of time and never overnight. Special category data (e.g. SEND, safeguarding, health data) must be kept on the staff member's person at all times.
    iii. Special category data must be returned to our premises at the end of the working day. If this is not practicable, and a staff member needs to retain the information in their personal possession, this must be discussed in advance with a member of SLT including what measures will be taken to safeguard the information, given the risks that are beyond a staff member's control in so doing and the potential consequences ensuing. The relevant member of the SLT must record their decision.
    iv. Data will be tidied away when not in use (e.g. when staff undertake working at home, it must be out of sight of family members, not left out, and tidied away).
    v. Only those who have need to access the data concerned will be granted permission and access to it.
    vi. Our data security policy / acceptable use / remote working policies describe the requirements around bring your own device, remote working and password protection.
  - **Accountability –** The Stonehenge School complies with its obligations under data protection laws including the UK GDPR and can demonstrate this via the measures set out in this policy including completing data protection impact assessments (DPIAs) where necessary; integrating data protection into internal documents including this policy, any related policies and privacy notices; regularly training members of staff on all relevant data protection law, including this and any related policies; reviewing and auditing privacy measures and compliance; maintaining and reviewing records of its processing activities

for all personal data that it holds; reviewing and ensuring familiarity of policies related to the handling of data; reviewing reasons for data breaches; and ensuring stakeholders manage risks and compliance using the annual compliance statement.

## 9. Processing Personal Data

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

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

### 9.1. Processing Special Categories of Personal Data

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

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

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

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

d) Processing is carried out in the course of its legitimate activities by a **not-for-profit organisation** with a political, philosophical, religious, or trade union aim on the condition that the processing relates solely to its members, or former member who have regular contact with it, and that the personal data are not disclosed outside that body without consent.

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

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

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

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

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

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

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

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

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

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

### 9.2. Legal basis for processing criminal offence data

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

We do not maintain a register of criminal convictions.

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

- The processing is necessary for the purposes of performing or exercising obligations or rights which are imposed or conferred by law on the controller or the individual in connection with employment, social security or social protection;
- The processing is necessary for the purposes of protecting the physical, mental or emotional well-being of an individual;
- The processing is necessary for statutory purposes; or
- Consent – where freely given. We acknowledge because of the potential for the imbalance of power that it may be difficult for consent to be deemed valid and will only rely on this where no other grounds apply.

## 10. Third Parties with Access to Personal Data

Please refer to our privacy notices for details of who, aside from The Stonehenge School, has access to the personal data processed.

### 10.1. Data Sharing

The Stonehenge School will only share personal data under limited circumstances, when there is a lawful basis to do so and where identified in the Privacy Notice(s). The following principles apply:

- We will share data if there is an issue with an individual or parent/carer that puts the safety of staff or others at risk;
- We will share data where there is a need to liaise with other agencies. We will seek consent as necessary and appropriate before doing so. However, where child protection and safeguarding concerns apply, we will apply the "Seven golden rules of information sharing." In limited circumstances, data may be shared with external agencies without the knowledge or consent of the parent or child in line with the DPA 2018, which includes 'safeguarding of children and individuals at risk' as a condition that allows practitioners to share information without consent;

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

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

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

### 10.2. Third-Party Processors

The Stonehenge School's suppliers and contractors, including its Data Protection Officer and IT provider, may need access to data to provide services. When third parties are processing personal data on behalf of us, we will:

- Only appoint suppliers or contractors who can provide sufficient guarantees that they comply with data protection law;
- Establish a data processing contract with the supplier or contractor, either in the contract or as a standalone agreement, to ensure the fair and lawful processing of any personal data dislosed;
- Only provide access to data that the supplier or contractor needs to carry out their service, and information necessary to keep them safe while working.

## 11. Data Protection by Design and Default

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

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

## 12. Personal data breaches or near misses

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

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

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

### Biometric Recognition Systems

Biometric data consists of personal information about an individual's physical or behavioural characteristics which may be used to identify that person. It may take the form of fingerprint, voice, or facial recognition. We use biometric data for our cashless catering system only (thumb print readers).

We will undertake a data protection impact assessment before implementing any new biometric system to assess the impact on individuals.

In the case of adults, for example staff members, we will seek their consent direct from them before processing any biometric data.

In accordance with the Protection of Freedoms Act 2012, in the case of children, we will notify all those will parental responsibility in the case of any individual under 18, unless this is impractical (for example the whereabouts of the parent is unknown or if there is a safeguarding issue) and may only proceed if we have at least one positive written consent, and no written parental objection. We will not proceed to process the information if the child themselves objects. Either parents or the child may withdraw their consent at any time.

If the individual concerned does not agree to proceed or wishes to withdraw their consent to the use of the biometric system, we will provide an alternative means of achieving the same aim.

## 13. Destruction of records

We adhere to our retention policy and will permanently securely destroy both paper and electronic records securely in accordance with these timeframes.

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

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

## 14. Training

To meet its obligations under data protection legislation, we will ensure that all staff, volunteers, and governors receive an appropriate level of data protection training as part of their induction. Permanent members of staff will receive data protection training annually. Those who have a need for additional training will be provided with it, for example relating to use of systems or CCTV.

Data protection also forms part of continuing professional development. Staff members undertake regular informal discussions on data protection, to ensure key updates are provided where changes to legislation, guidance or our processes make it necessary. This will include lessons learned from data breaches and near misses, preventative measures to avoid them, and other best practice as advised.

## 15. Monitoring Arrangements

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

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

## 16. Complaints

The Stonehenge School is always seeking to implement best practice and strives for the highest standards. We operate an "open door" policy to discuss any concerns about the implementation of this policy or related issues. Our Complaints Policy can be found on our website.

Individuals have the right to make a complaint to us about the way in which we process personal data. There is also a right to make a complaint to the Information Commissioner, but complaints should be raised with us first by contacting dpo@stonehenge.wilts.sch.uk We will acknowledge your complaint within 30 days and respond without undue delay.

The ICO is contactable at:

www.ico.org.uk

Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF

Telephone: 0303 123 1113

## 17. Legislation and Guidance

This policy takes into account the following:

- The UK General Data Protection Regulation (UK GDPR)
- The Data Protection Act (DPA) 2018
- The Data (Use and Access) Act 2025 (DUAA)
- The Protection of Freedoms Act 2012
- Guidance published by the Information Commissioner's Office
- Information Sharing – Advice for Practitioners – DfE July 2018.

## 18. Links with Other Policies

This Data Protection Policy is linked to the following:

- Information Security Policy
- Retention & Disposal / Records Management Policy
- Data Breach Policy
- Privacy Notices
- Safeguarding Policy
- Acceptable Usage Policies
- E-Safety/Online Safety Policy
- Consent / Permissions Form
- Admissions Form

## 19. Approval

This policy was approved by The Stonehenge School Governing Body on 29th Jan 2026

## Appendix 1 – Examples of Special Category Data that we process

Employee health data and information concerning their racial / ethnic origin

Pupil health data and information concerning their racial / ethnic origin in admissions records and in pupil records / trip packs

Special Educational Needs information

School census information

Attendance records

Biometric data e.g. fingerprints for cashless catering / door entry systems

Information contained within child protection and safeguarding records

Staff application forms

HR files including and disciplinary and capability proceedings which may include DBS, and right to work checks, health, and equal opportunities data (disability, race, ethnicity, sexual orientation).

Accident reporting documentation

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

# Data Protection Policy

## Appendix 2 – Subject Access Request Procedure (SAR)

The Stonehenge School shall complete the following steps when processing a request for personal data (Subject Access Request or SAR) with advice from its Data Protection Officer (One West).

1. Ascertain whether the requester has a right to access the information and capacity.
2. Obtain (reasonable and proportionate) proof of identity.
3. Engage with the requester if the request needs clarifying.

   Nb only once steps 2 and 3 have been completed, can the "clock" start.
4. Make a judgement on whether the request is complex and therefore can be extended by an additional two months.
5. Acknowledge the requester providing them with
   a. the response time – one calendar month (as standard), an additional two months if complex; and
   b. details of any costs – free for standard requests, or we can charge, or refuse to process, if the request is manifestly unfounded or excessive, or further copies of duplicate information is required, the fee must be in line with the administrative cost.
6. Use its Record of Processing Activities and/or data map to identify data sources and where they are held.
7. Collect the data (the organisation may use its IT support to pull together electronic data sources such as emails and databases).
8. If (6) identifies third parties who process it, then engage with them to release the data to The Stonehenge School.
9. Review the identified data for exemptions and redactions in line with the ICO's Guide to the Right of Access and in consultation with the organisation's Data Protection Officer (One West).
10. Create the final bundle and check to ensure all redactions have been applied.
11. Submit the final bundle to the requester in a secure manner and in the format they have requested.