SESSET

Data Protection Policy

Approved by:	**Trustees**	**Date:** July 2023
Last reviewed on:	**July 2022**	**Created:** 22nd May 2018
Next review due by:	Summer term 2024	

Contents

1. Aims

Our school aims to ensure that all personal data collected about staff, students, parents, governors, visitors and other individuals is collected, stored and processed in accordance with the General Data Protection Regulation (UK-GDPR) and the provisions of the Data Protection Act 2018 (DPA 2018) as set out in the Data Protection Bill.

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-GDPR and the provisions of the DPA 2018. It is based on guidance published by the Information Commissioner's Office (ICO) on the UK GDPR and the ICO's code of practice for subject access requests.

It meets the requirements of the Protection of Freedoms Act 2012 when referring to our use of biometric data.

It also reflects the ICO's code of practice for the use of surveillance cameras and personal information. In addition, this policy complies with our funding agreement and articles of association. This policy complies with regulation 5 of the Education (Pupil Information) (England) Regulations 2005, which gives parents the right of access to their child's educational record.

3. Definitions

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.

Term	Definition
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

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

SESSET processes personal data relating to parents, students, staff, governors, visitors and others, and therefore is a data controller.

5. Roles and responsibilities

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

5.1 Governing board and SESSET Trustees

The governing board of each school has overall responsibility for ensuring that its school complies with all relevant data protection obligations.

5.2 Data Protection Officer

The Trust's 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.

They will provide an annual report of their activities directly to the governing 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.

Full details of the DPO's responsibilities are set out in their job description.

The Trust's DPO reports directly to the Trust's Executive Headteacher and is supported by DPLs in each school.

Our DPO is Mr James Robinson and is contactable via robinson.james@ashcombe.surrey.sch.uk or at The Ashcombe School, Ashcombe Road, Dorking, Surrey, RH4 1LY (01306 886312).

The DPO is supported by Data Protection Leads in each of the schools – Mr Ben Stafford, Carrington School, and Mr M Houghton, Therfield School.

5.3 Headteacher

The school's headteacher acts as the representative of the data controller on a day-to-day basis.

5.4 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 or DPL 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 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
    - they have any other questions or concerns relating to the processing of data.

6. Data protection principles

6.1 In accordance with the requirements outlined in the UK-GDPR, personal data will be:

- processed lawfully, fairly and in a transparent manner in relation to individuals
- collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be incompatible with the initial purposes
- accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data, which is inaccurate, having regard to the purposes for which they are processed, is erased, or rectified without delay
- kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods, insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, subject to implementation of the appropriate technical and organisational measures required by the UK-GDPR in order to safeguard the rights and freedoms of individuals
- processed in a manner that ensures appropriate security of personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction, or damage, using appropriate technical or organisational measures

6. 2. The UK-GDPR also requires that "the controller shall be responsible for, and able to demonstrate, compliance with the principles".

7. Collecting personal data

7.1 Lawfulness, fairness and transparency

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

- 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 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 student) has freely given clear **consent.**

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

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

Whenever we first collect personal data directly from individuals, we will provide them with the relevant information required by data protection law.

7.2 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.

Staff must only process personal data where it is necessary to do their jobs.

When staff no longer need the personal data they hold, they must ensure it is deleted or anonymised. This will be done in accordance with the Trust's Data Retention Policy.

8. Sharing personal data

We will not normally share personal data with anyone else unless this is required to meet the needs of the Trust's Privacy Notices.

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

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

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

When we transfer personal data to a country or territory outside the European Economic Area, we will 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
- 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 must be submitted in writing, either by letter, email or fax to the DPO. They should include:

- name of individual
- correspondence address
- 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.

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 students at our school may not be granted without the express permission of the student. This is not a rule and a student'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, we:

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

We will not disclose information if it:

- might cause serious harm to the physical or mental health of the student 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 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.

9.4 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:

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

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

10. Parental requests to see the educational record

Parents, or those with parental responsibility, are able to request access to their child's educational record (which includes most information about a student) and, where this is possible, we will aim to respond within 1 month of receipt of a written request.

This should be formally requested from the DPO.

11. Biometric recognition systems

Where we use students' biometric data as part of an automated biometric recognition system (for example, students use finger prints to receive school dinners instead of paying with 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 get written consent from at least one parent or carer before we take any biometric data from their child and first process it.

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

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

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

Where staff members or other adults use the school's biometric system(s), we will also obtain their consent before they first take part in it, and provide alternative means of accessing the relevant service if they object. Staff and other adults can also withdraw consent at any time, and the school will delete any relevant data already captured.

12. CCTV

We use CCTV in various locations around the school site to protect the school premises and to ensure it remains safe. We will adhere to the ICO's code of practice for the use of CCTV.

We do not need to ask individuals' permission to use CCTV, but security cameras are clearly visible. Any enquiries about the CCTV system should be directed to the school's Facilities Manager.

13. 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, or students aged 18 and over, for photographs and videos to be taken of students for communication, marketing and promotional materials.

Where we need parental consent, we will clearly explain how the photograph and/or video will be used to both the parent/carer and student. Where we don't need parental consent, we will clearly explain to the student how the photograph and/or video will be used.

Uses may include:

- Within school on noticeboards 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 child, to ensure they cannot be identified.

14. Data protection by design and default

The school will act in accordance with the UK-GDPR by adopting a privacy by design approach and implementing technical and organisational measures which demonstrate how the college has considered and integrated data protection into 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 (see section 6)
- carrying out Data protection impact assessments (DPIAs). These will be used to identify the most effective method of complying with the College's data protection obligations and meeting individuals' expectations of privacy. A DPIA will be carried out when using new technologies or when the processing is likely to result in a high risk to the rights and freedoms of individuals.
- completing privacy 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 will 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; we will also keep a record of attendance
- regularly conducting reviews and audits to test our privacy measures and make sure we are 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 and all information we are required to share about how we use and process their personal data (via our privacy notices)

- For all personal data that we hold, maintaining an internal record of the type of data, data subject, how and why we are using the data, any third-party recipients, how and why we are storing the data, retention periods and how we are keeping the data secure. All data should be retained no longer than necessary. Retention periods for different data types will be reviewed on an annual basis and adhere to national guidelines from the DfE and ICO.

15. 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:

- Software patches will be applied to MIS systems to enhance data security and update data records. Software patches which alter data records will be considered by the DPO and the Deputy DPOs from the three schools.
- Double factor authentication is installed on all web facing systems.
- Digital data is encrypted or password-protected, both on a local hard drive and on a network drive that is regularly backed up off-site.
- All electronic devices are password-protected to protect the information on the device in case of theft.
- Confidential paper records will be kept in a locked filing cabinet, drawer or safe, with restricted access.
- Confidential paper records will not be left unattended or in clear view anywhere with general access.
- All necessary members of staff are provided with their own secure login and password.
- Circular emails to parents/carers are sent via our internal communication systems which ensure that email addresses are not disclosed to other recipients.
- Parents are not included in the CC address field in emails.
- Where personal information that could be considered private or confidential is taken off the premises, either in electronic or paper format, staff will take extra care to follow the same procedures for security, e.g. keeping devices under lock and key.
- The person taking the information from the school premises accepts full responsibility for the security of the data.
- Before sharing data, all staff members will ensure:
  - they are allowed to share it.
  - that adequate security is in place to protect it.
- Under no circumstances are visitors allowed access to confidential or personal information. Visitors to areas of the school containing sensitive information are supervised at all times.
- The physical security of the school's buildings and storage systems, and access to them, is reviewed on a termly basis. If an increased risk in vandalism/burglary/theft is identified, extra measures to secure data storage will be put in place.
- The school takes its duties under the UK-GDPR seriously and any unauthorised disclosure may result in disciplinary action.
- The Network Manager is responsible for continuity and recovery measures are in place to ensure the security of protected data.

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 we cannot or do not need to rectify or update it.

For example, we will shred or incinerate paper-based records, and overwrite or delete electronic files. 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.

17. 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 in appendix 1.

When appropriate, we will report the data breach to the ICO within 72 hours.

18. Training

All staff, governors, and trustees are provided with the relevant data protection training as related to their role.

Data protection will also form part of continuing professional development, where changes to legislation, guidance or the school's processes make it necessary.

19. Monitoring arrangements

The DPO is responsible for monitoring and reviewing this policy and will work with school headteachers and trustees on these reviews.

This policy will be reviewed every 2 years and shared with the trustees and local governing boards. We will change the policy in response to changes in the law regarding data protection.

20. Links with other policies

This data protection policy is linked to our:

- Freedom of information publication scheme
- Data Retention Policies
- SESSET Staff Code of Conduct
- ICT Usage Policies.

Appendix 1: Personal data breach procedure

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

- On finding or causing a breach, or potential breach, the staff member or data processor must immediately notify the DPO.
- The DPO will investigate the report and determine whether a breach has occurred. To decide, 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
    - Made available to unauthorised people.
- The DPO will alert the headteacher and the chairs of governors and Trustees.
- 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. (Actions relevant to specific data types are set out at the end of this procedure.)
- The DPO will assess the potential consequences, based on how serious they are, and how likely they are to happen.
- The DPO will work out 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.

  If it is likely that there will be a risk to people's rights and freedoms, the DPO must notify the ICO.
- The DPO will document the decision (either way), in case it is challenged at a later date by the ICO or an individual affected by the breach. Documented decisions are stored on The Ashcombe SharePoint network.
- 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.
- If all the above details are not yet known, the DPO will report as much as they can 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.

- 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 promptly inform, in writing, all 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, or will be, taken to deal with the data breach and mitigate any possible adverse effects on the individual(s) concerned.
- 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.
- The DPO will document each breach, irrespective of whether it is reported to the ICO. For each breach, this record will include the:
    - facts and cause
    - effects
    - 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 stored on Ashcombe's computer system.
- The DPO and headteacher will meet to review what happened and how it can be stopped from happening again. This meeting will happen as soon as reasonably possible.

Actions to minimise the impact of data breaches

We will take actions to mitigate the impact of different types of data breach, focusing especially on breaches involving particularly risky or sensitive information. We will review the effectiveness of these actions and amend them as necessary after any data breach.