



Data protection Policy

**Southwood, Downs Barn and Germander Park
Schools**

Reviewed: September 2024

Approved by BPP Governors: September 2024

To be reviewed: September 2026

Contents

1. Aims	2
2. Legislation and guidance.....	2
3. Definitions.....	3
4. The data controller	4
5. Roles and responsibilities.....	4
6. Data protection principles.....	5
7. Collecting personal data.....	5
8. Sharing personal data	6
9. Subject access requests and other rights of individuals	7
10. Parental requests to see the educational record	9
11. Biometric recognition systems.....	9
12. CCTV.....	9
13. Photographs and videos.....	10
14. Artificial intelligence (AI).....	11
15. Data protection by design and default.....	11
16. Data security and storage of records	11
17. Disposal of records	12
18. Personal data breaches	12
19. Training.....	12
20. Monitoring arrangements	12
21. Links with other policies	12
Appendix 1: Personal data breach procedure.....	13

1. Aims

Our school aims to ensure that all personal data collected about staff, pupils, parents and carers, governors, 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 the [UK GDPR](#) and guidance from the Department for Education (DfE) on [Generative artificial intelligence in education](#).

Formatted: Not Highlight

Formatted: Not Highlight

Formatted: Not Highlight

Schools that use biometric data insert:

It meets the requirements of the [Protection of Freedoms Act 2012](#) when referring to our use of biometric data.

Schools that use CCTV insert:

It also reflects the ICO's [guidance](#) for the use of surveillance cameras and personal information.

Maintained schools, pupil referral units (PRUs) and non-maintained special schools add:

In addition, 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.

Academies, including free schools, if applicable, add/amend:

In addition, this policy complies with our funding agreement and articles of association.

3. Definitions

TERM	DEFINITION
Personal data	<p>Any information relating to an identified, or identifiable, living individual.</p> <p>This may include the individual's:</p> <ul style="list-style-type: none">› Name (including initials)› Identification number› Location data› Online identifier, such as a username <p>It may also include factors specific to the individual's physical, physiological, genetic, mental, economic, cultural or social identity.</p>
Special categories of personal data	<p>Personal data which is more sensitive and so needs more protection, including information about an individual's:</p> <ul style="list-style-type: none">› Racial or ethnic origin› Political opinions› Religious or philosophical beliefs› Trade union membership› Genetics› Biometrics (such as fingerprints, retina and iris patterns), where used for identification purposes› Health – physical or mental› Sex life or sexual orientation
Processing	<p>Anything done to personal data, such as collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing or destroying.</p> <p>Processing can be automated or manual.</p>
Data subject	<p>The identified or identifiable individual whose personal data is held or processed.</p>
Data controller	<p>A person or organisation that determines the purposes and the means of processing personal data.</p>

Formatted: Not Highlight

TERM	DEFINITION
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

Our school processes personal data relating to parents and carers, pupils, staff, governors, visitors and others, and therefore is a data controller.

The school ~~is registered with the ICO / has paid its data protection fee to the ICO, and will pay this annually or as otherwise legally required. (Delete as applicable.)~~

Formatted: English (United Kingdom), Pattern: Clear

Formatted: English (United Kingdom), Pattern: Clear

Formatted: 1 body copy 10pt

Formatted: English (United Kingdom), Pattern: Clear, Highlight

Formatted: English (United Kingdom), Pattern: Clear

Formatted: English (United Kingdom), Pattern: Clear

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

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

5.2 Data protection officer (DPO)

The data protection officer (DPO) is responsible for overseeing the implementation of this policy, monitoring our compliance with data protection law, and developing related policies and guidelines where applicable.

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.

For routine enquiries about this policy, contact the school's data protection representative in the first instance: Mrs Kate Mathews, Headteacher.

Our DPO is ~~name~~The ICT Service and is contactable via ~~contact details~~ DPO@theictservice.org.uk.

Formatted: English (United Kingdom)

Formatted: 1 body copy 10pt

~~If your school has a data protection lead in addition to your DPO, for example because your DPO is outsourced and so you need a staff member to manage data protection day-to-day, you can add details here about their role and what they're responsible for.~~

Formatted: English (United Kingdom), Highlight

Formatted: English (United Kingdom)

Formatted: English (United Kingdom)

5.3 Headteacher

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

Formatted: 1 body copy 10pt

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 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 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 our school must comply with.

Formatted: Not Highlight

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

We will only process personal data where we have 1 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 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 or another person i.e. 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 public 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**

For special categories of personal data, we will also meet 1 of the special category conditions for processing under data protection law:

- › The individual (or their parent/carer when appropriate in the case of a pupil) has given **explicit consent**

- › The data needs to be processed to perform or exercise obligations or rights in relation to **employment, social security or social protection law**
- › The data needs to be processed to ensure the **vital interests** of the individual or another person, where the individual is physically or legally incapable of giving consent
- › The data has already been made **manifestly public** by the individual
- › The data needs to be processed for the establishment, exercise or defence of **legal claims**
- › The data needs to be processed for reasons of **substantial public interest** as defined in legislation
- › The data needs to be processed for **health or social care purposes**, and the processing is done by, or under the direction of, a health or social work professional or by any other person obliged to confidentiality under law
- › The data needs to be processed for **public health reasons**, and the processing is done by, or under the direction of, a health professional or by any other person obliged to confidentiality under law
- › The data needs to be processed for **archiving purposes**, scientific or historical research purposes, or statistical purposes, and the processing is in the public interest

For criminal offence data, we will meet both a lawful basis and a condition set out under data protection law. Conditions include:

- › The individual (or their parent/carer when appropriate in the case of a pupil) has given **consent**
- › The data needs to be processed to ensure the **vital interests** of the individual or another person, where the individual is physically or legally incapable of giving consent
- › The data has already been made **manifestly public** by the individual
- › The data needs to be processed for or in connection with legal proceedings, to obtain legal advice, or for the establishment, exercise or defence of **legal rights**
- › The data needs to be processed for reasons of **substantial public interest** as defined in legislation

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

We will always consider the fairness of our data processing. We will ensure we do not handle personal data in ways that individuals would not reasonably expect, or use personal data in ways which have unjustified adverse effects on them.

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 in order to do their jobs.

We will keep data accurate and, where necessary, up to date. Inaccurate data will be rectified or erased when appropriate.

In addition, 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 [school's record retention schedule](#) **Retention Schedule set out in the Information and Record Management Society's Toolkit for Schools. This can be found in the Appendix.**

Formatted: 1 body copy 10pt

Formatted: English (United States)

8. Sharing personal data

We will not normally share personal data with anyone else without consent, but there are certain circumstances where we may be required to do so. These include, but are not limited to, situations where:

Formatted: Not Highlight

- There is an issue with a pupil or parent/carer that puts the safety of our staff at risk
- We need to liaise with other agencies – we will seek consent as necessary before doing this
- Our suppliers or contractors need data to enable us to provide services to our staff and pupils – for example, IT companies. When doing this, we will:
 - Only appoint suppliers or contractors that can provide sufficient guarantees that they comply with UK data protection law
 - Establish a contract with the supplier or contractor to ensure the fair and lawful processing of any personal data we share
 - Only share data that the supplier or contractor needs to carry out their service

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

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

Where we transfer personal data internationally, we will do so in accordance with UK 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 can be submitted in any form, but we may be able to respond to requests more quickly if they are made in writing and include:

- Name of individual
- Correspondence address
- Contact number and email address
- Details of the information requested

If staff receive a subject access request in any form they must immediately forward it to [the DPO Mrs Kate Mathews, Headteacher](#).

9.2 Children and subject access requests

Formatted: 1 body copy 10pt

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.

Primary schools add:

Children below the age of 12 are generally not 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 our school may 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.

Secondary schools add:

~~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 our 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, 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 (or receipt of the additional information needed to confirm identity, where relevant)
- 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

Formatted: Not Highlight

We may not disclose information for a variety of reasons, such as if it:

- Might cause serious harm to the physical or mental health of the pupil or another individual
- Would reveal that the child is being or has been abused, or is at risk of abuse, where the disclosure of that information would not be in the child's best interests
- Would include another person's personal data that we can't reasonably anonymise, and we don't have the other person's consent 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, we may refuse to act on it, or charge a reasonable fee to cover administrative costs. We will take into account whether the request is repetitive in nature when making this decision.

Formatted: Not Highlight

When we refuse a request, we will tell the individual why, and tell them they have the 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 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 (in certain circumstances)
- Prevent use of their personal data for direct marketing
- Object to processing that has been justified on the basis of public interest, official authority or legitimate interests

Formatted: Not Highlight

- Challenge decisions based solely on automated decision making or profiling (i.e. making decisions or evaluating certain things about an individual based on their personal data with no human involvement)
- 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-contact the school's data protection representative in the first instance. Mrs Kate Mathews, Headteacher](#). If staff receive such a request, they must immediately forward it to [contact the school's data protection representative or](#) the DPO.

Formatted: 1 body copy 10pt, Indent: Left: 0 cm

10. Parental requests to see the educational record

~~All maintained schools, pupil referral units and non-maintained special schools insert:~~

Parents, or those with parental responsibility, have a legal right to free access to their child's educational record (which includes most information about a pupil) within 15 school days of receipt of a written request.

If the request is for a copy of the educational record, the school may charge a fee to cover the cost of supplying it.

This right applies as long as the pupil concerned is aged under 18.

There are certain circumstances in which this right can be denied, such as if releasing the information might cause serious harm to the physical or mental health of the pupil or another individual, or if it would mean releasing exam marks before they are officially announced.

~~Academies, including free schools, and independent schools: there is no automatic parental right of access to the educational record in your setting, but you may choose to provide this. Set out your school's approach, explain whether charges apply, and explain how parents/carers can make a request.~~

11. Biometric recognition systems

~~If your school uses, or plans to Southwood, Downs Barn and Germander Park Schools do not use, any biometric recognition systems, insert the text below. If not, delete this whole section and re-number the remaining sections.~~

Formatted: Highlight

Formatted: Highlight

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

~~Where we use pupils' biometric data as part of an automated biometric recognition system (for example, pupils use finger prints to receive school dinners instead of paying with cash [amend this example as applicable]), 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 1 parent or carer before we take any biometric data from their child and first process it all.~~

Formatted: 1 body copy 10pt

Formatted: English (United Kingdom)

~~Parents/carers and pupils 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 pupils. For example, pupils can pay for school dinners in cash at each transaction if they wish [amend this example as applicable].~~

~~Parents/carers and pupils can withdraw consent, at any time, and we 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, we will not process that data irrespective of any consent given by the pupil's parent(s)/carer(s).~~

~~Add if applicable:~~

~~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.~~

Formatted: 1 body copy 10pt

12. CCTV

~~If your school uses CCTV, insert the text below. If not, delete this whole section and re-number the remaining sections.~~

Formatted: English (United Kingdom)

We use CCTV in various locations around the school site to ensure it remains safe. We will follow the [ICO's guidance](#) for the use of CCTV, and comply with data protection principles.

Formatted: Not Highlight

We do not need to ask individuals' permission to use CCTV, but we make it clear where individuals are being recorded. Security cameras are clearly visible and accompanied by prominent signs explaining that CCTV is in use.

Any enquiries about the CCTV system should be directed to [\[name/job title\]-Mrs Kate Mathews, Headteacher.](#)

13. Photographs and videos

As part of our school activities, we may take photographs and record images of individuals within our school.

~~Primary schools insert:~~

We will obtain written consent from parents/carers for photographs and videos to be taken of their child for communication, marketing and promotional materials. We will clearly explain how the photograph and/or video will be used to both the parent/carer and the pupil.

Any photographs and videos taken by parents/carers at school events for their own personal use are not covered by data protection legislation. However, we will ask that photos or videos with other pupils are not shared publicly on social media for safeguarding reasons, unless all the relevant parents/carers have agreed to this.

~~Secondary schools insert:~~

~~We will obtain written consent from parents/carers, or pupils aged 18 and over, for photographs and videos to be taken of pupils 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 the pupil. Where we don't need parental consent, we will clearly explain to the pupil how the photograph and/or video will be used.~~

~~Any photographs and videos taken by parents/carers at school events for their own personal use are not covered by data protection legislation. However, we will ask that photos or videos with other pupils are not shared publicly on social media for safeguarding reasons, unless all the relevant parents/carers (or pupils where appropriate) have agreed to this.~~

~~All schools add and adapt to reflect your school's uses of photographs and videos for communication, marketing and promotional materials:~~

Where the school takes photographs and videos, uses may include:

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

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

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

~~Insert, if relevant:~~

See our [child protection and safeguarding policy/photography policy/other relevant policy](#) for more information on our use of photographs and videos.

14. Artificial intelligence (AI)

Artificial intelligence (AI) tools are now widespread and easy to access. Staff, pupils and parents/carers may be familiar with generative chatbots such as ChatGPT and Google Bard. [\[School or trust name\]](#) recognises [The BPP Schools recognise](#) that AI has many uses to help pupils learn, but also poses risks to sensitive and personal data.

To ensure that personal and sensitive data remains secure, no one will be permitted to enter such data into unauthorised generative AI tools or chatbots.

If personal and/or sensitive data is entered into an unauthorised generative AI tool, [\[school/trust name\]](#) [the BPP schools](#) will treat this as a data breach, and will follow the personal data breach procedure outlined in appendix 1.

15. Data protection by design and default

We will put measures in place to show that we have integrated data protection into all of our 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 (see section 6)
- 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 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
- Appropriate safeguards being put in place if we transfer any personal data outside of the UK, where different data protection laws may apply
- 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, type of data subject, how and why we are using the data, any third-party recipients, any transfers outside of the UK and the safeguards for those, retention periods and how we are keeping the data secure

16. 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:

- Paper-based records and portable electronic devices, such as laptops and hard drives that contain personal data, are kept under lock and key when not in use

Formatted: English (United Kingdom)

Formatted: English (United Kingdom), Highlight

Formatted: English (United Kingdom), Highlight

Formatted: English (United Kingdom)

Formatted: 1 body copy 10pt

Formatted: Not Highlight

Formatted: Not Highlight

Formatted: Not Highlight

- Papers containing confidential personal data must not be left on office and classroom desks, on staffroom tables, or left anywhere else where there is general access
- Where personal information needs to be taken off site, staff must sign it in and out from the school office
- Passwords that are at least 10 characters long containing letters and numbers are used to access school computers, laptops and other electronic devices. Staff and pupils are reminded that they should not reuse passwords from other sites
- Encryption software is used to protect all portable devices and removable media, such as laptops and USB devices
- Staff, pupils or governors who store personal information on their personal devices are expected to follow the same security procedures as for school-owned equipment (see our acceptable use policy)
- Where we need to share personal data with a third party, we carry out due diligence and take reasonable steps to ensure it is stored securely and adequately protected (see section 8)

17. 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.

All data will be kept in accordance with the Retention Schedule set out in the Information and Record Management Society's Toolkit for Schools. This can be found in the Appendix.

18. 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 after becoming aware of it. Such breaches in a school context may include, but are not limited to:

- A non-anonymised dataset being published on the school website, which shows the exam results of pupils eligible for the pupil premium
- Safeguarding information being made available to an unauthorised person
- The theft of a school laptop containing non-encrypted personal data about pupils

19. Training

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

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

20. Monitoring arrangements

The Headteacher and DPO are responsible for monitoring and reviewing this policy.

This policy will be reviewed every two years and approved by the full governing board.

21. Links with other policies

This data protection policy is linked to our:

- Freedom of information publication scheme
- Privacy notices

Appendix 1: Personal data breach procedure

This procedure is based on [guidance on personal data breaches](#) produced by the Information Commissioner's Office (ICO).

- On finding or causing a breach or potential breach, the staff member, governor or data processor must immediately notify Mrs Kate Mathews by email, who will inform the data protection officer (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
- Staff and governors will co-operate with the investigation (including allowing access to information and responding to questions). The investigation will not be treated as a disciplinary investigation
- If a breach has occurred or it is considered to be likely that is the case, the DPO will alert the headteacher and the chair of governors
- The DPO will make all reasonable efforts to contain and minimise the impact of the breach. Relevant staff members or data processors should help the DPO with this where necessary, and the DPO should take external advice when required (e.g. from IT providers). (See the actions relevant to specific data types 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) before and after the implementation of steps to mitigate the consequences
- The DPO will work out whether the breach must be reported to the ICO and the individuals affected using the ICO's [self-assessment tool](#)
- The DPO will document the decisions (either way), in case the decisions are challenged at a later date by the ICO or an individual affected by the breach. Documented decisions are stored on the Google Drive in the MLT folder.
- 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. 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 of the school's awareness of the breach. 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
- Where the school is required to communicate with individuals whose personal data has been breached, the DPO will tell them in writing. This notification will set out:

- A description, in clear and plain language, of the nature of the personal data breach
 - 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 consider, 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
- 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 the Google Drive in the MLT folder.

- 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
- The DPO and headteacher will meet regularly to assess recorded data breaches and identify any trends or patterns requiring action by the school to reduce risks of future breaches

Actions to minimise the impact of data breaches

We set out below the steps we might take to try and mitigate the impact of different types of data breach if they were to occur, 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.

Sensitive information being disclosed via email (including safeguarding records)

- If special category data (sensitive information) is accidentally made available via email to unauthorised individuals, the sender must attempt to recall the email as soon as they become aware of the error
- Members of staff who receive personal data sent in error must alert the sender and the DPO as soon as they become aware of the error
- If the sender is unavailable or cannot recall the email for any reason, the DPO will ask the [ICT department/external IT support provider] to attempt to recall it from external recipients and remove it from the school's email system (retaining a copy if required as evidence)
- In any cases where the recall is unsuccessful or cannot be confirmed as successful, the DPO will consider whether it's appropriate to contact the relevant unauthorised individuals who received the email, explain that the information was sent in error, and request that those individuals delete the information and do not share, publish, save or replicate it in any way
- The DPO will endeavor to obtain a written response from all the individuals who received the data, confirming that they have complied with this request
- The DPO will carry out an internet search to check that the information has not been made public; if it has, we will contact the publisher/website owner or administrator to request that the information is removed from their website and deleted
- If safeguarding information is compromised, the DPO will inform the designated safeguarding lead and discuss whether the school should inform any, or all, of its 3 local safeguarding partners

Other types of breach that you might want to consider could include:

- Details of pupil premium interventions for named children being published on the school website
- Non-anonymised pupil exam results or staff pay information being shared with governors

- A school laptop containing non-encrypted sensitive personal data being stolen or hacked
- The school's cashless payment provider being hacked and parents' financial details stolen
- Hardcopy reports sent to the wrong pupils or families



Privacy notice for staff

Under data protection law, individuals have a right to be informed about how the school uses any personal data that we hold about them. We comply with this right by providing privacy notices to individuals where we are processing their personal data.

This privacy notice explains how we collect, store and use personal data about individuals we employ, or otherwise engage, to work at our school.

We, Southwood School, Bryony Place, Conniburrow, Milton Keynes, MK14 7AR, Downs Barn School, 69 Downs Barn Boulevard, Downs Barn, Milton Keynes MK14 7NA and Germander Park School, 1 Germander Place, Conniburrow, Milton Keynes, MK14 7DU, are the 'data controller' for the purposes of data protection law.

Our Data Protection Officer is The ICT Service and is contactable via DPO@theictservice.org.uk

The personal data we hold

We process data relating to those we employ, or otherwise engage, to work at our school. Personal data that we may collect, use, store and share (when appropriate) about you includes, but is not restricted to:

- Full name, date of birth, marital status and gender
- Address and contact details
- Next of kin and emergency contact numbers
- Salary, annual leave, pension and benefits information
- Bank account details, payroll records, National Insurance number and tax status information
- Recruitment information, including copies of right to work documentation, references and other information included in a CV or cover letter or as part of the application process
- Qualifications and employment records, including work history, job titles, working hours, training records and professional memberships
- Performance information
- Outcomes of any disciplinary and/or grievance procedures
- Absence data
- Copy of driving licence
- Photographs
- CCTV footage
- Data about your use of the school's information and communications system

We may also collect, store and use information about you that falls into "special categories" of more sensitive personal data. This includes information about (where applicable):

- Race, ethnicity, religious beliefs, sexual orientation and political opinions
- Trade union membership
- Health, including any medical conditions, and sickness records

Why we use this data

The purpose of processing this data is to help us run the school, including to:

- Enable you to be paid
- Facilitate safe recruitment, as part of our safeguarding obligations towards pupils
- Support effective performance management
- Inform our recruitment and retention policies
- Allow better financial modelling and planning
- Enable ethnicity and disability monitoring
- Improve the management of workforce data across the sector
- Support the work of the School Teachers' Review Body

Our lawful basis for using this data

We only collect and use personal information about you when the law allows us to. Most commonly, we use it where we need to:

- Fulfil a contract we have entered into with you
- Comply with a legal obligation
- Carry out a task in the public interest

Less commonly, we may also use personal information about you where:

- You have given us consent to use it in a certain way
- We need to protect your vital interests (or someone else's interests)

Where you have provided us with consent to use your data, you may withdraw this consent at any time. We will make this clear when requesting your consent, and explain how you go about withdrawing consent if you wish to do so.

Some of the reasons listed above for collecting and using personal information about you overlap, and there may be several grounds which justify the school's use of your data.

Collecting this information

While the majority of information we collect from you is mandatory, there is some information that you can choose whether or not to provide to us.

Whenever we seek to collect information from you, we make it clear whether you must provide this information (and if so, what the possible consequences are of not complying), or whether you have a choice.

How we store this data

We create and maintain an employment file for each staff member. The information contained in this file is kept secure and is only used for purposes directly relevant to your employment.

Once your employment with us has ended, we will retain this file and delete the information in it in accordance with the Retention Schedule set out in the school's retention policy, available from the school office.

Data sharing

We do not share information about you with any third party without your consent unless the law and our policies allow us to do so.

Where it is legally required, or necessary (and it complies with data protection law) we may share personal information about you with:

- Our local authority – to meet our legal obligations to share certain information with it, such as safeguarding concerns and information about headteacher performance and staff dismissals
- The Department for Education – to meet our legal obligations
- Your family or representatives – to fulfil our contractual obligations
- Educators and examining bodies – to fulfil our public task
- Our regulator Ofsted – to meet our legal obligations and fulfil our public task
- Suppliers and service providers – to enable them to provide the service we have contracted them for, such as payroll
- Our auditors – to meet our legal obligations
- Security organisations – to fulfil our contractual obligations and to ensure the security of the pupils in school
- Health and social welfare organisations – to meet our legal obligations through our recruitment process
- Professional advisers and consultants – to fulfil our public task in providing training opportunities to staff to improve work performance
- Police forces, courts, tribunals – to meet legal obligations
- Employment and recruitment agencies – to fulfil our legal and contractual obligations

Transferring data internationally

Where we transfer personal data to a country or territory outside **the United Kingdom**, we will do so in accordance with data protection law.

Your rights

How to access personal information we hold about you

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

If you make a subject access request, and if we do hold information about you, we will:

- Give you a description of it
- Tell you why we are holding and processing it, and how long we will keep it for
- Explain where we got it from, if not from you
- Tell you who it has been, or will be, shared with
- Let you know whether any automated decision-making is being applied to the data, and any consequences of this
- Give you a copy of the information in an intelligible form

You may also have the right for your personal information to be transmitted electronically to another organisation in certain circumstances.

If you would like to make a request, please contact Mrs Kate Mathews, Headteacher, Southwood School 01908 678366, office@southwoodschool.co.uk, Downs Barn School 01908 604430 office@downsbarnschool.co.uk and Germander Park School, 01908 674620 office@germanderpark.com

Your other rights regarding your data

Under data protection law, individuals have certain rights regarding how their personal data is used and kept safe. You have the right to:

- Object to the use of your personal data if it would cause, or is causing, damage or distress
- Prevent your data being used to send direct marketing
- Object to the use of your personal data for decisions being taken by automated means (by a computer or machine, rather than by a person)
- In certain circumstances, have inaccurate personal data corrected, deleted or destroyed, or restrict processing
- Claim compensation for damages caused by a breach of the data protection regulations

To exercise any of these rights, please contact Mrs Kate Mathews, Headteacher, Southwood School 01908 678366, office@southwoodschool.co.uk, Downs Barn School 01908 604430 office@downsbarnschool.co.uk and Germander Park School, 01908 674620 office@germanderpark.com

Complaints

We take any complaints about our collection and use of personal information very seriously.

If you think that our collection or use of personal information is unfair, misleading or inappropriate, or have any other concern about our data processing, please raise this with us in the first instance.

To make a complaint, please contact Mrs Kate Mathews, Headteacher, Southwood School 01908 678366, office@southwoodschool.co.uk, Downs Barn School 01908 604430 office@downsbarnschool.co.uk and Germander Park School, 01908 674620 office@germanderpark.com

You can also contact our Data Protection Officer (The ICT Service):

Email: DPO@theictservice.org.uk

Tel: 0300 300 0000

Address: Speke House, 17 Compass Point Business Park, Stocks Bridge Way, St Ives, Cambs PE27 5JL

Alternatively, you can make a complaint to the Information Commissioner's Office:

- Report a concern online at <https://ico.org.uk/concerns/>
- Call 0303 123 1113
- Or write to: Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF

Contact us

If you have any questions, concerns or would like more information about anything mentioned in this privacy notice, please contact:

Mrs Kate Mathews, Headteacher, Southwood School 01908 678366, office@southwoodschool.co.uk, Downs Barn School 01908 604430 office@downsbarnschool.co.uk and Germander Park School, 01908 674620 office@germanderpark.com.

This notice is based on the [Department for Education's model privacy notice](#) for the school workforce, amended to reflect the way we use data in this school.



Privacy notice for pupils

Under data protection law, individuals have a right to be informed about how the school uses any personal data that we hold about them. We comply with this right by providing privacy notices to individuals where we are processing their personal data.

This privacy notice explains how we collect, store and use personal data about **pupils**.

We, Southwood, Downs Barn and Germander Park schools, are the 'data controller' for the purposes of data protection law.

Our DPO is The ICT Service and is contactable via DPO@theictservice.org.uk.

The personal data we hold

Personal data that we may collect, use, store and share (when appropriate) about students/pupils includes, but is not restricted to:

- Contact details, contact preferences, date of birth, identification documents
- Results of internal assessments and externally set tests
- Pupil and curricular records
- Characteristics, such as ethnic background, eligibility for free school meals, or special educational needs
- Exclusion information
- Behaviour information
- Details of any medical conditions, including physical and mental health
- Attendance information
- Safeguarding information
- Details of any support received, including care packages, plans and support providers
- Photographs
- CCTV images captured in school
- Data about use of the school's information and communications system

We may also hold data about students/pupils that we have received from other organisations, including other schools, local authorities and the Department for Education.

Why we use this data

We use this data to:

- Support student/pupil learning
- Monitor and report on student/pupil progress
- Provide appropriate pastoral care

- Protect student/pupil welfare
- Assess the quality of our services
- Administer admissions waiting lists
- Carry out research
- Comply with the law regarding data sharing

Our legal basis for using this data

We only collect and use pupils' personal data when the law allows us to. Most commonly, we process it where:

- We need to comply with a legal obligation
- We need it to perform an official task in the public interest

Less commonly, we may also process pupils' personal data in situations where:

- We have obtained consent to use it in a certain way
- We need to protect the individual's vital interests (or someone else's interests)

Where we have obtained consent to use pupils' personal data, this consent can be withdrawn at any time. We will make this clear when we ask for consent, and explain how consent can be withdrawn.

Some of the reasons listed above for collecting and using pupils' personal data overlap, and there may be several grounds which justify our use of this data.

Collecting this information

While the majority of information we collect about pupils is mandatory, there is some information that can be provided voluntarily.

Whenever we seek to collect information from you or your child, we make it clear whether providing it is mandatory or optional. If it is mandatory, we will explain the possible consequences of not complying.

How we store this data

We keep personal information about students/pupils while they are attending our school. We may also keep it beyond their attendance at our school if this is necessary in order to comply with our legal obligations. We keep personal data according to the Retention Schedule set out in the school's retention policy, available from the school office.

Data sharing

We do not share information about pupils with any third party without consent unless the law and our policies allow us to do so.

Where it is legally required, or necessary (and it complies with data protection law) we may share personal information about pupils with:

- Our local authority – to meet our legal obligations to share certain information with it, such as safeguarding concerns and exclusions
- The Department for Education – to meet our legal obligations to share certain information with it.
- The pupil's family and representatives – to provide regular reports on the pupil's progress and to ensure the pupil's safety whilst at school
- Educators and examining bodies – to meet our legal obligations and allow the pupil to be entered for assessments
- Ofsted – to meet our legal obligations
- Suppliers and service providers – to enable them to provide the service we have contracted them for

- Survey and research organisations – to help us fulfil our public task
- Health authorities – to meet our legal obligation to keep our pupils safe
- Health and social welfare organisations – to meet our legal obligation and to protect the pupils
- Professional advisers and consultants – to help us fulfil our public task
- Charities and voluntary organisations - to help us fulfil our public task and to protect the pupils
- Police forces, courts, tribunals – to meet our legal obligations to share information with them

Transferring data internationally

Where we transfer personal data to a country or territory outside **the United Kingdom**, we will do so in accordance with data protection law.

National Pupil Database

We are required to provide information about pupils to the Department for Education as part of statutory data collections such as the school census and early years' census.

Some of this information is then stored in the [National Pupil Database](#) (NPD), which is owned and managed by the Department for Education and provides evidence on school performance to inform research.

The database is held electronically so it can easily be turned into statistics. The information is securely collected from a range of sources including schools, local authorities and exam boards.

The Department for Education may share information from the NPD with other organisations which promote children's education or wellbeing in England. Such organisations must agree to strict terms and conditions about how they will use the data.

For more information, see the Department's webpage on [how it collects and shares research data](#).

You can also [contact the Department for Education](#) with any further questions about the NPD.

Parents and pupils' rights regarding personal data

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

Parents/carers can make a request with respect to their child's data where the child is not considered mature enough to understand their rights over their own data (usually under the age of 12), or where the child has provided consent.

Parents also have the right to make a subject access request with respect to any personal data the school holds about them.

If you make a subject access request, and if we do hold information about you or your child, we will:

- Give you a description of it
- Tell you why we are holding and processing it, and how long we will keep it for
- Explain where we got it from, if not from you or your child
- Tell you who it has been, or will be, shared with
- Let you know whether any automated decision-making is being applied to the data, and any consequences of this
- Give you a copy of the information in an intelligible form

Individuals also have the right for their personal information to be transmitted electronically to another organisation in certain circumstances.

Parents/carers also have a legal right to access to their child's **educational record**. To request access, please contact Mrs Kate Mathews, Headteacher, Southwood School 01908 678366, office@southwoodschool.co.uk, Downs Barn School 01908 604430 office@downsbarnschool.co.uk and Germander Park School, 01908 674620 office@germanderpark.com.

Other rights

Under data protection law, individuals have certain rights regarding how their personal data is used and kept safe, including the right to:

- Object to the use of personal data if it would cause, or is causing, damage or distress
- Prevent it being used to send direct marketing
- Object to decisions being taken by automated means (by a computer or machine, rather than by a person)
- In certain circumstances, have inaccurate personal data corrected, deleted or destroyed, or restrict processing
- Claim compensation for damages caused by a breach of the data protection regulations

To exercise any of these rights, please contact Mrs Kate Mathews, Headteacher, Southwood School 01908 678366, office@southwoodschool.co.uk, Downs Barn School 01908 604430 office@downsbarnschool.co.uk and Germander Park School, 01908 674620 office@germanderpark.com.

Complaints

We take any complaints about our collection and use of personal information very seriously.

If you think that our collection or use of personal information is unfair, misleading or inappropriate, or have any other concern about our data processing, please raise this with us in the first instance.

To make a complaint, please contact Mrs Kate Mathews, Headteacher, Southwood School 01908 678366, office@southwoodschool.co.uk, Downs Barn School 01908 604430 office@downsbarnschool.co.uk and Germander Park School, 01908 674620 office@germanderpark.com.

You can also contact our Data Protection Officer (The ICT Service):

Email: DPO@theictservice.org.uk

Tel: **0300 300 0000**

Address: Speke House, 17 Compass Point Business Park, Stocks Bridge Way, St Ives, Cambs PE27 5JL

Alternatively, you can make a complaint to the Information Commissioner's Office:

- Report a concern online at <https://ico.org.uk/concerns/>
- Call 0303 123 1113
- Or write to: Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF

Contact us

If you have any questions, concerns or would like more information about anything mentioned in this privacy notice, please contact:

Mrs Kate Mathews, Headteacher, Southwood School 01908 678366, office@southwoodschool.co.uk, Downs Barn School 01908 604430 office@downsbarnschool.co.uk and Germander Park School, 01908 674620 office@germanderpark.com.

This notice is based on the [Department for Education's model privacy notice for pupils](#), amended to reflect the way we use data in this school.



Privacy notice for parents/carers

Under data protection law, individuals have a right to be informed about how the school uses any personal data that we hold about them. We comply with this right by providing privacy notices to individuals where we are processing their personal data.

This privacy notice explains how we collect, store and use personal data about **parents**.

We, Southwood, Downs Barn and Germander Park schools, are the 'data controller' for the purposes of data protection law.

Our DPO is The ICT Service and is contactable via DPO@theictservice.org.uk.

The personal data we hold

Personal data that we may collect, use, store and share (when appropriate) about parents may include, but is not restricted to:

- Name, address and date of birth,
- Contact details, contact preferences, identification documents
- Characteristics such as ethnic background, first language
- Employment details such as place of work, occupation, job title, NI number
- Whether there is a court order in place restricting the parent's access to their child

We may also hold data about parents that we have received from other organisations, including other schools, local authorities and the Department for Education.

Why we use this data

We use this data to:

- Provide appropriate pastoral care
- Protect student/pupil welfare
- Administer admissions waiting lists
- Comply with the law regarding data sharing

Our legal basis for using this data

We only collect and use parents' personal data when the law allows us to. Most commonly, we process it where:

- We need to comply with a legal obligation
- We need it to perform an official task in the public interest

Less commonly, we may also process parents' personal data in situations where:

- We have obtained consent to use it in a certain way
- We need to protect the individual's vital interests (or someone else's interests)

Where we have obtained consent to use parents' personal data, this consent can be withdrawn at any time. We will make this clear when we ask for consent, and explain how consent can be withdrawn.

Some of the reasons listed above for collecting and using parents' personal data overlap, and there may be several grounds which justify our use of this data.

Collecting this information

While the majority of information we collect about parents is mandatory, there is some information that can be provided voluntarily.

Whenever we seek to collect information from you, we make it clear whether providing it is mandatory or optional. If it is mandatory, we will explain the possible consequences of not complying.

How we store this data

We keep personal information about students/pupils and their parents while they are attending our school. We may also keep it beyond their attendance at our school if this is necessary in order to comply with our legal obligations. We store this data in both digital and paper based formats. We keep personal data according to the Retention Schedule set out in the school's retention policy, available from the school office.

Data sharing

We do not share information about parents with any third party without consent unless the law and our policies allow us to do so.

Where it is legally required, or necessary (and it complies with data protection law) we may share personal information about parents with:

- Our local authority – to meet our legal obligations to share certain information with it, such as safeguarding concerns and exclusions
- The Department for Education – to meet our legal obligations to share certain information with it.
- Suppliers and service providers – to enable them to provide the service we have contracted them for
- Survey and research organisations – to help us fulfil our public task
- Health authorities – to meet our legal obligation to keep our pupils safe
- Health and social welfare organisations – to meet our legal obligation and to protect our pupils
- Charities and voluntary organisations - to help us fulfil our public task and to protect the pupils
- Police forces, courts, tribunals – to meet our legal obligations to share information with them

Transferring data internationally

Where we transfer personal data to a country or territory outside **the United Kingdom**, we will do so in accordance with data protection law.

Parents' rights regarding personal data

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

If you make a subject access request, and if we do hold information about you, we will:

- Give you a description of it
- Tell you why we are holding and processing it, and how long we will keep it for
- Explain where we got it from, if not from you or your child
- Tell you who it has been, or will be, shared with
- Let you know whether any automated decision-making is being applied to the data, and any consequences of this
- Give you a copy of the information in an intelligible form

Individuals also have the right for their personal information to be transmitted electronically to another organisation in certain circumstances.

Other rights

Under data protection law, individuals have certain rights regarding how their personal data is used and kept safe, including the right to:

- Object to the use of personal data if it would cause, or is causing, damage or distress
- Prevent it being used to send direct marketing
- Object to decisions being taken by automated means (by a computer or machine, rather than by a person)
- In certain circumstances, have inaccurate personal data corrected, deleted or destroyed, or restrict processing
- Claim compensation for damages caused by a breach of the data protection regulations

To exercise any of these rights, please contact Mrs Kate Mathews, Headteacher, Southwood School 01908 678366, office@southwoodschool.co.uk, Downs Barn School 01908 604430 office@downsbarnschool.co.uk and Germander Park School, 01908 674620 office@germanderpark.com.

Complaints

We take any complaints about our collection and use of personal information very seriously.

If you think that our collection or use of personal information is unfair, misleading or inappropriate, or have any other concern about our data processing, please raise this with us in the first instance.

To make a complaint, please contact Mrs Kate Mathews, Headteacher, Southwood School 01908 678366, office@southwoodschool.co.uk, Downs Barn School 01908 604430 office@downsbarnschool.co.uk and Germander Park School, 01908 674620 office@germanderpark.com.

You can also contact our Data Protection Officer (The ICT Service):

Email: DPO@theictservice.org.uk

Tel: 0300 300 0000

Address: Speke House, 17 Compass Point Business Park, Stocks Bridge Way, St Ives, Cambs PE27 5JL

Alternatively, you can make a complaint to the Information Commissioner's Office:

- Report a concern online at <https://ico.org.uk/concerns/>
- Call 0303 123 1113
- Or write to: Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF

Contact us

If you have any questions, concerns or would like more information about anything mentioned in this privacy notice, please contact:

Mrs Kate Mathews, Headteacher, Southwood School 01908 678366, office@southwoodschool.co.uk, Downs Barn School 01908 604430 office@downsbarnschool.co.uk and Germander Park School, 01908 674620 office@germanderpark.com.

This notice is based on the [Department for Education's model privacy notice](#) for pupils, amended for parents and to reflect the way we use data in this school.



Privacy Notice for Governors/Trustees and Volunteers

Under data protection law, individuals have a right to be informed about how Southwood School, Bryony Place, Conniburrow, Milton Keynes, MK14 7AR, Downs Barn School, 69 Downs Barn Boulevard, Downs Barn, Milton Keynes MK14 7NA and Germander Park School, 1 Germander Place, Conniburrow, Milton Keynes, MK14 7DU uses any personal data held about them. We comply with this right by providing privacy notices to individuals where we are processing their personal data.

This privacy notice explains how we collect, store and use personal data about individuals applying for jobs at our school.

We, Southwood, Downs Barn and Germander Park Schools are the 'data controller' for the purposes of data protection law.

Our DPO is The ICT Service and is contactable via DPO@theictservice.org.uk.

The personal data we hold

We process data relating to those volunteering at our school. Personal data that we may collect, use, store and share (when appropriate) about you includes, but is not restricted to:

- Full name and address
- Contact details
- References
- Evidence of qualifications
- Employment details
- Information about business and pecuniary interests

We may also collect, store and use information about you that falls into "special categories" of more sensitive personal data. This may include information about (where applicable):

- Race, ethnicity, religious beliefs, sexual orientation and political opinions
- Disability and access requirements

Why we use this data

The purpose of processing this data is to support the school to:

- Establish and maintain effective governance
- Meet statutory obligations for publishing and sharing Governors' details
- Facilitate safe recruitment, as part of our safeguarding obligations towards pupils
- Undertake equalities monitoring
- Ensure that appropriate access arrangements can be provided for volunteers who require them

Our lawful basis for using this data

We only collect and use personal information about you when the law allows us to. Most commonly, we use it where we need to:

- Comply with a legal obligation
- Carry out a task in the public interest

Less commonly, we may also use personal information about you where:

- You have given us consent to use it in a certain way
- We need to protect your vital interests (or someone else's interests)

Where you have provided us with consent to use your data, you may withdraw this consent at any time. We will make this clear when requesting your consent and explain how you go about withdrawing consent if you wish to do so.

Some of the reasons listed above for collecting and using personal information about you overlap, and there may be several grounds which justify our use of your data.

Collecting this information

While most of the information we collect from you is mandatory, there is some information that you can choose whether or not to provide to us.

Whenever we seek to collect information from you, we make it clear whether you must provide this information (and if so, what the possible consequences are of not complying), or whether you have a choice.

How we store this data

Personal data we collect as part of the application process is stored in line with Southwood, Downs Barn and Germander Park schools' Data Protection and GDPR Policy.

We maintain a file to store personal information about all volunteers. The information contained in this file is kept secure and is only used for purposes directly relevant to your work with the school.

Once your relationship with us has ended, we will retain this file and delete the information in it in accordance with the Retention Schedule set out in the school's retention policy, available from the school office.

Data sharing

We do not share information about you with any third party without your consent unless the law and our policies allow us to do so.

Where it is legally required, or necessary (and it complies with data protection law) we may share personal information about you with:

- Government departments or agencies – to meet our legal obligations to share information about governors/trustees
- Our local authority – to meet our legal obligations to share certain information with it, such as details of governors
- Suppliers and service providers – to enable them to provide the service we have contracted them for, such as governor/trustee support
- Professional advisers and consultants
- Employment and recruitment agencies
- Police forces, courts

Transferring data internationally

Where we transfer personal data to a country or territory outside **the United Kingdom**, we will do so in accordance with data protection law.

Use of your personal information for marketing purposes

Where you have given us consent to do so, the school may send you marketing information by e-mail or text promoting school events, campaigns, charitable causes or services that may be of interest to you. You can "opt out" of receiving these texts and/or e-mails at any time by clicking on the "Unsubscribe" link at the bottom of any such communication, or by contacting our data protection officer.

Your rights

How to access the personal information we hold about you

Individuals have a right to make a 'subject access request' to gain access to personal information that we hold about them.

If you make a subject access request, and if we do hold information about you, we will:

- Give you a description of it
- Tell you why we are holding and processing it, and how long we will keep it for
- Explain where we got it from, if not from you
- Tell you who it has been, or will be, shared with
- Let you know whether any automated decision-making is being applied to the data, and any consequences of this

- Give you a copy of the information in an intelligible form

You may also have a right for your personal information to be transmitted electronically to another organisation in certain circumstances.

If you would like to make a request, please contact Mrs Kate Mathews, Headteacher, Southwood School 01908 678366, office@southwoodschool.co.uk, Downs Barn School 01908 604430 office@downsbarnschool.co.uk and Germander Park School, 01908 674620 office@germanderpark.com

Your other rights regarding your data

Under data protection law, individuals have certain rights regarding how their personal data is used and kept safe. You have the right to:

- Object to the use of your personal data if it would cause, or is causing, damage or distress
- Prevent your data being used to send direct marketing
- Object to the use of your personal data for decisions being taken by automated means (by a computer or machine, rather than a person)
- In certain circumstances, have inaccurate personal data corrected, deleted or destroyed, or restrict processing
- Claim compensation for damages caused by a breach of the data protection regulations

To exercise any of these rights, please contact Mrs Kate Mathews, Headteacher, Southwood School 01908 678366, office@southwoodschool.co.uk, Downs Barn School 01908 604430 office@downsbarnschool.co.uk and Germander Park School, 01908 674620 office@germanderpark.com

Complaints

We take any complaints about our collection and use of personal information very seriously.

If you think that our collection or use of personal information is unfair, misleading or inappropriate, or have any other concern about our data processing, please raise this with us in the first instance.

To make a complaint, please contact Mrs Kate Mathews, Headteacher, Southwood School 01908 678366, office@southwoodschool.co.uk, Downs Barn School 01908 604430 office@downsbarnschool.co.uk and Germander Park School, 01908 674620 office@germanderpark.com.

You can also contact our Data Protection Officer (The ICT Service):

Email: DPO@theictservice.org.uk

Tel: 0300 300 0000

Address: Speke House, 17 Compass Point Business Park, Stocks Bridge Way, St Ives, Cambs PE27 5JL

Alternatively, you can make a complaint to the Information Commissioner's Office:

- Report a concern online at <https://ico.org.uk/concerns/>
- Call 0303 123 1113
- Or write to: Information Commissioner's Office, Wycliff House, Water Lane, Wilmslow, Cheshire, SK9 5AF

Contact us

If you have any questions, concerns or would like more information about anything mentioned in this privacy notice, please contact:

Mrs Kate Mathews, Headteacher, Southwood School 01908 678366, office@southwoodschool.co.uk, Downs Barn School 01908 604430 office@downsbarnschool.co.uk and Germander Park School, 01908 674620 office@germanderpark.com

This notice is based on the [Department for Education's model privacy notice](#) for governors and volunteers amended to reflect the way we use data in the school.



Privacy Notice for Job Applicants

Under data protection law, individuals have a right to be informed about how Southwood School, Bryony Place, Conniburrow, Milton Keynes, MK14 7AR, Downs Barn School, 69 Downs Barn Boulevard, Downs Barn, Milton Keynes MK14 7NA and Germander Park School, 1 Germander Place, Conniburrow, Milton Keynes, MK14 7DU uses any personal data held about them. We comply with this right by providing privacy notices to individuals where we are processing their personal data.

This privacy notice explains how we collect, store and use personal data about individuals applying for jobs at our school.

We, Southwood, Downs Barn and Germander Park Schools are the 'data controller' for the purposes of data protection law.

Our DPO is The ICT Service and is contactable via DPO@theictservice.org.uk.

Successful candidates should refer to our privacy notice for the school workforce for information about how their personal data is collected, stored and used during their period of employment.

The personal data we hold

We process data relating to those applying to work at, Southwood and Downs Barn Schools. Personal data that we may collect, use, store and share (when appropriate) about you includes, but is not restricted to:

- Full name and address
- Contact details
- Copies of right to work documentation
- References
- Evidence of qualifications
- Employment records, including work history, job titles, training records and professional memberships

We may also collect, store and use information about you that falls into "special categories" of more sensitive personal data. This includes information about (where applicable):

- Race, ethnicity, religious beliefs, sexual orientation and political opinions
- Disability and access requirements

Why we use this data

The purpose of processing this data is to aid the recruitment process by:

- Enabling us to establish relevant experience and qualifications
- Facilitating safe recruitment, as part of our safeguarding obligations towards pupils
- Enabling equalities monitoring
- Ensuring that appropriate access arrangements can be provided for candidates that require them

Our lawful basis for using this data

We only collect and use personal information about you when the law allows us to. Most commonly, we use it where we need to:

- Comply with a legal obligation
- Carry out a task in the public interest

Less commonly, we may also use personal information about you where:

- You have given us consent to use it in a certain way

- We need to protect your vital interests (or someone else's interests)
- Where you have provided us with consent to use your data, you may withdraw this consent at any time. We will make this clear when requesting your consent and explain how you go about withdrawing consent if you wish to do so.

Some of the reasons listed above for collecting and using personal information about you overlap, and there may be several grounds which justify the Trust's use of your data.

Collecting this information

While most of the information we collect from you is mandatory, there is some information that you can choose whether or not to provide to us.

Whenever we seek to collect information from you, we make it clear whether you must provide this information (and if so, what the possible consequences are of not complying), or whether you have a choice.

How we store this data

Personal data we collect as part of the job application process is stored in line with Southwood, Downs Barn and Germander Park schools' Data Protection and GDPR Policy.

We will retain, and dispose of, the personal data of all unsuccessful job applicants in accordance with the Retention Schedule set out in the school's retention policy, available from the school office.

Data sharing

We do not share information about you with any third party without your consent unless the law and our policies allow us to do so.

Where it is legally required, or necessary (and it complies with data protection law), we may share personal information about you with:

- Our local authority – to meet our legal obligations to share certain information with it, such as shortlists of candidates for a headteacher position
- Suppliers and service providers – to enable them to provide the service we have contracted them for, such as HR and recruitment support
- Professional advisers and consultants
- Employment and recruitment agencies

Transferring data internationally

Where we transfer personal data to a country or territory outside **the United Kingdom**, we will do so in accordance with data protection law.

Your rights

How to access the personal information we hold about you

Individuals have a right to make a 'subject access request' to gain access to personal information that the Trust holds about them.

If you make a subject access request, and if we do hold information about you, we will:

- Give you a description of it
- Tell you why we are holding and processing it, and how long we will keep it for
- Explain where we got it from, if not from you
- Tell you who it has been, or will be, shared with
- Let you know whether any automated decision-making is being applied to the data, and any consequences of this

- Give you a copy of the information in an intelligible form

You may also have a right for your personal information to be transmitted electronically to another organisation in certain circumstances.

If you would like to make a request, please contact Mrs Kate Mathews, Headteacher, Southwood School 01908 678366, office@southwoodschool.co.uk, Downs Barn School 01908 604430 office@downsbarnschool.co.uk and Germander Park School, 01908 674620 office@germanderpark.com

Your other rights regarding your data

Under data protection law, individuals have certain rights regarding how their personal data is used and kept safe. You have the right to:

- Object to the use of your personal data if it would cause, or is causing, damage or distress
- Prevent your data being used to send direct marketing
- Object to the use of your personal data for decisions being taken by automated means (by a computer or machine, rather than a person)
- In certain circumstances, have inaccurate personal data corrected, deleted or destroyed, or restrict processing
- Claim compensation for damages caused by a breach of the data protection regulations

To exercise any of these rights, please contact Mrs Kate Mathews, Headteacher, Southwood School 01908 678366, office@southwoodschool.co.uk, Downs Barn School 01908 604430 office@downsbarnschool.co.uk and Germander Park School, 01908 674620 office@germanderpark.com.

Complaints

We take any complaints about our collection and use of personal information very seriously.

If you think that our collection or use of personal information is unfair, misleading or inappropriate, or have any other concern about our data processing, please raise this with us in the first instance.

To make a complaint, please contact Mrs Kate Mathews, Headteacher, Southwood School 01908 678366, office@southwoodschool.co.uk, Downs Barn School 01908 604430 office@downsbarnschool.co.uk and Germander Park School, 01908 674620 office@germanderpark.com

You can also contact our Data Protection Officer (The ICT Service):

Email: DPO@theictservice.org.uk

Tel: 0300 300 0000

Address: Speke House, 17 Compass Point Business Park, Stocks Bridge Way, St Ives, Cambs PE27 5JL

Alternatively, you can make a complaint to the Information Commissioner's Office:

- Report a concern online at <https://ico.org.uk/concerns/>
- Call 0303 123 1113
- Or write to: Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF

Contact us

If you have any questions, concerns or would like more information about anything mentioned in this privacy notice, please contact:

Mrs Kate Mathews, Headteacher, Southwood School 01908 678366, office@southwoodschool.co.uk, Downs Barn School 01908 604430 office@downsbarnschool.co.uk and Germander Park School, 01908 674620 office@germanderpark.com.

This notice is based on the [Department for Education's model privacy notice for staff](#), amended to reflect the way we use data in this school.



Southwood, Downs Barn and Germander Park Schools'

Data Retention Information

Reviewed By: Kate Mathews/ Carrie Matthews	Date: September 2024
Review:	Date: September 2026

Data Item Group	Short term (event + 1 month)	Medium term (pupil at school + 1 year)	Long term (pupil at school + 6 years)	Very long term (until pupil is aged 25 or older)	Comment
Admissions		X	X (appeals)		Used extensively from point of arrival to point of leaving. Used to validate and cross check information. Data kept 1 year after leaving to allow for enquiries and appeals.
Attainment			X		Summative attainment kept to enable schools to understand and analyse previous attainment (trend analysis). Also retained for 1 year for enquiries from other schools the child may move to.
Attendance			X		Attendance data only relevant whilst the child is on roll. Kept 1 + year for enquiries only.
Behaviour		X			School term + one year to allow for a period of handover with the receiving school.
Exclusions		X			School term + one year to allow for a period of handover with the receiving school. This then becomes their responsibility.

Identity management and authentication		X			Photo of child attached to mis records to assist staff in recognising individuals *NB MIS system currently retains photos indefinitely. This is under review.
Catering and Free School Meal Management	X (meal administration)		X (FSM eligibility info)		FSM info linked to funding and therefore comes under the 7 year financial retention guidelines.
Trip and Activities	X (registers, or risk assessments for visitors in school)	X permissions from parents	X (financial info)	X (if major medical event)	All significant medical records must be kept until the child reaches 25 years of age.
Medical Information and Administration	X (permission slips)	X (medical conditions and ongoing management)		X (medical incidents)	Medical incidents would be deemed as those with behaviour or welfare/safeguarding link or any incident that required significant treatment off site.
Safeguarding				X	Safeguarding information is passed on securely to receiving schools. It will be kept when a receiving school has not been identified
SEND (special needs)		X		X if unable to pass files to receiving school	
Personal Identifiers, contacts and personal characteristics		X (images used in displays in school) X (house number and road)	X (postcodes) X (names) X (characteristics) X (images used in school marketing materials)		Some items kept for data and trend analysis e.g. postcodes, number of free school meals etc.
School Finance inc. Lettings, Fund etc.			X (7 years for all school financial records)		

School Personnel		X (all details)	X (basic details)		This additional retention allows for reference requests
Governors' Minutes				X life of the school	Do not contain personal data. Kept securely on Governor Hub
Governors' Reports			X		
Allegations against staff				X	10 years or until retirement, whichever is longer
Visitor records including volunteers, work experience etc.	X general visitors		X work experience		
School Insurance details				X 40 years	
Newsletters etc.		X			1 year
Meeting minutes (SLT)			X 5 years		
Site management records including risk assessments etc.			X 7 years		
Asbestos management				X 40 years	
Historical Log Books of school history				X life of school	