# Data Protection Policy

| | |
|---|---|
| Owner: | David Powell |
| Date Ratified: | October 9th 2025 |
| Ratified by: | FGB |
| Date Policy to be reviewed: | Autumn 2026 |

## 1. Aims

Our school aims to ensure that all personal data collected about staff, pupils, parents, governors, visitors and other individuals is collected, stored and processed in accordance with the General Data Protection Regulation (GDPR) and the expected 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 expected provisions of the DPA 2018. It is based on guidance published by the Information Commissioner's Office (ICO) on the GDPR and the ICO's code of practice for subject access requests. It also reflects the ICO's code of practice for the use of surveillance cameras and personal information. 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.

## 3. Definitions

| Term | Definition |
|---|---|
| Personal data | Any information relating to an identified, or identifiable, individual.<br>This may include the individual's:<br>• Name (including initials)<br>• Identification number<br>• Location data<br>• Online identifier, such as a username<br>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:<br>Racial or ethnic origin<br>• Political opinions<br>• Religious or philosophical beliefs<br>• Trade union membership<br>• Genetics<br>• Biometrics (such as fingerprints, retina and iris patterns), where used for identification purposes<br>• Health – physical or mental<br>• Sex life or sexual orientation |
| Processing | Anything done to personal data, such as collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing or destroying.<br><br>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

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

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

## 5. Roles and Responsibilities

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

### Governing Body

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

### Data Protection Officer

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 body 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. Our DPO a third party company, Turn it On and they are contactable via the school office. The Business Manager or IT and Data Manager will be the person to contact in the first instance and will liaise with the DPO.

### Business Manager and IT and Data Manager

The Business Manager and IT and Data Manager act as the representatives of the data controller on a day to-day basis.

### Staff – all 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 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; With any contracts or sharing personal data with third parties

## 6. Data Protection Principles

The GDPR is based on data protection principles that our school must comply with. The principles say that personal data must be:

Processed lawfully, fairly and in a transparent manner
Collected for specified, explicit and legitimate purposes
Adequate, relevant and limited to what is necessary to fulfil the purposes for which it is processed
Accurate and, where necessary, kept up to date
Kept for no longer than is necessary for the purposes for which it is processed
Processed in a way that ensures it is appropriately secure

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

## 7. Collecting Personal Data

### 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. These lawful bases are: The data needs to be processed so that the school can fulfil a contract with the individual, or the individual has asked the school to take specific steps before entering into a contract; The data needs to be processed so that the school can comply with a legal obligation; The data needs to be processed to ensure the vital interests of the individual e.g. to protect someone's life; The data needs to be processed so that the school, as a public authority, can perform a task in the public interest, 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 pupil) 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/or Data Protection Act 2018.

If we offer online services to pupils, such as classroom apps, and we intend to rely on consent as a basis for processing, we will obtain parental consent unless it is required for the school to undertake its function under one of the legal bases outlined above.

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

**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.

When staff no longer need the personal data they hold, they must ensure it is deleted. This will be done in accordance with the record retention appendix of this policy.

## 8. Sharing Personal Data

We will not normally share personal data with anyone else, but may do so where:

- 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 unless it is required for the school to undertake its function under one of the legal bases outlined above.

Our suppliers or contractors need data to enable us to provide services to our staff and pupils. When doing this, we will: Only appoint suppliers or contractors which can provide sufficient guarantees that they comply with data protection law; Establish a data sharing agreement with the supplier or contractor, either in the contract or as a standalone agreement, to ensure the fair and lawful processing of any personal data we share; Only share data that the supplier or contractor needs to carry out their service, and information necessary to keep them safe while working with us

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 situation that affects any of our pupils or staff.

Where 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

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 or email 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 Business Manager, IT and Data Manager and/or DPO.

### 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 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.

### Responding to subject access requests

When responding to requests, we:

- Will ask the individual to provide 1 form of identification.
- Will contact the individual via phone to confirm the request was made.
- Will respond without delay and within 30 days of receipt of the request.
- Will provide the information free of charge.
- May tell the individual we will comply within 90 days of receipt of the request, where a request is complex or numerous. We will inform the individual of this within 30 days, 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 pupil or another individual
- Would reveal that the child is at risk of abuse, where the disclosure of that information would not be in the child's best interests
- Is contained in adoption or parental order records
- Is given to a court in proceedings concerning the child

If the request is unfounded or excessive, we may refuse to act on it, or charge a reasonable fee which 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.

**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 of the 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 an authorised 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. If staff receive such a request, they must immediately forward it to the Executive Business Manager, IT and Data Manager and/or DPO.

## 10. Parental Requests to see the Educational Record

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

## 11. CCTV

We use CCTV in various locations around the school's sites to ensure it remains safe. The use of CCTV is governed by the CCTV Policy. We will also 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 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 the Facilities Manager

## 12. Photographs and Videos

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

We will obtain consent from parents/carers for photographs and videos to be taken of their child for communication, marketing and promotional materials upon joining and periodically over a pupils time with the school. We will clearly explain how the photograph and/or video will be used to the parent/carer. Where we use photographs and recorded images as learning materials and for assessment we will not gain consent however will not share these photographs and/or recorded images without prior consent. Uses may include:

- 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. Where it is reasonable to do so, if consent is withdrawn, we will delete the photograph or video and not distribute it further.

## 13. 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 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
- It is a requirement of staff as part of their job descriptions to uphold the principles of GDPR and undertake data processing tasks within GDPR laws
- 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

## 14. 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 that contain personal data are kept under lock and key or behind electronic locks when not in use
- Digital devices that contain personal data are encrypted where they are portable or are secured by appropriate methods where they are fixed in position
- Papers containing confidential personal data must not be left on office and classroom desks, on staffroom tables, pinned to notice/display boards, or left anywhere else where there is general access
- Where personal information needs to be taken off site, staff will be aware of and comply with their GDPR duties to protect that data
- Passwords that comply with the schools' security recommendations are used to access their school accounts
- Portable storage devices will not be used to contain any Claycots School data
- Staff and governors will not use personal devices to store Claycots School data
- 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)

## 15. 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.

We will shred or incinerate paper-based records, and 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.

## 16. 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.

## 17. 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.

## 18. Monitoring Arrangements

The Business Manager, IT and Data Manager and DPO are responsible for monitoring and reviewing this policy.

This policy will be reviewed and updated if any changes are made to the law that affect our school's practice. Otherwise, this policy will be reviewed every 3 years and shared with the full governing body.

## 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 Executive Business Manager or IT and Data Manager who will inform the DPO if the breach is considered significant.
- The Executive Business Manager, IT and Data Manager and/or the DPO (referred to henceforth as 'the team') will investigate the report and determine whether a breach has occurred. To decide the team will consider whether personal data has been accidentally or unlawfully Lost, Stolen, Destroyed, Altered, Disclosed or made available where it should not have been or Made available to unauthorised people
- The team will alert the headteacher and the chair of governors
- The team 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 team will assess the potential consequences, based on how serious they are, and how likely they are to happen
- The team 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 team 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 o Discrimination; Identify theft or fraud; Financial loss; Unauthorised reversal of pseudonymisation (for example, key-coding); Damage to reputation o Loss of confidentiality; Any other significant economic or social disadvantage to the individual(s) concerned
- If it's likely that there will be a risk to people's rights and freedoms, the team must notify the ICO.
- The team 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 in electronic files kept by the team on the school network
- Where the ICO must be notified, the team will do this via the 'report a breach' page of the ICO website within 72 hours. As required, the team 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 team 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 team expects to have further information. The team will submit the remaining information as soon as possible
- The team 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 team 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 team 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 team 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 in electronic files kept by the team on the school network
- The team 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**

Both formal and informal risk assessments will take place to minimize the impact of any data breaches. Steps will be taken to reduce the risk should the event happen such a contacting a recipient of an email who is not the intended recipient of accidently shared personal information and barring access of a stolen mobile device to the school network both internally and externally.

## APPENDIX 2: 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' (sometimes called 'fair processing 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, Claycots School, are the 'data controller' for the purposes of data protection law.

Our data protection officer is provided by Turn IT On. (see 'Contact us' below).

### The personal data we hold

Personal data that we may collect, use, store and share (when appropriate) about 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
- Details of any medical conditions, including physical and mental health and allergy details
- Attendance information
- Safeguarding information
- Details of any support received, including care packages, plans and support providers
- Photographs
- CCTV images captured in school

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

### Why we use this data

We use this data to:

- Support pupil learning
- Monitor and report on pupil progress
- Provide appropriate pastoral care
- Protect pupil welfare
- Assess the quality of our services
- Administer admissions waiting lists
- Carry out research
- Comply with the law regarding data sharing
- Communicate effectively with parents/carers

### 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 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. Our record retention appendix of this policy sets out how long we keep information about pupils.

**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 and other local authorities where necessary – 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, such as safeguarding concerns and exclusions
- The pupil's family and representatives – to communicate effectively with our parents/carers
- Educators and examining bodies – to undertake statutory and non-statutory examinations to track and maximise the education of our pupils
- Our regulator Ofsted – to allow us to be inspected as an educational provider

- Suppliers and service providers – to enable them to provide the service we have contracted them for
- Financial organisations such as banks – to allow the school to manage its finances effectively.
- Our auditors – to allow the school to be proved to be working with integrity
- Health authorities – to allow our pupils and staff to access their services as and where required
- Health and social welfare organisations – to allow our pupils and staff to access their services as and where required
- Professional advisers and consultants– to allow our pupils and staff to access their services as and where required
- Police forces, courts, tribunals – to comply with law enforcement
- Professional bodies
- Educational providers and platforms we consider to enrich the education of the pupils.
- Limited AI platforms vetted and risk-assessed by the school to enhance the school's usual data processing activities.

**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.

Some of this information is then stored in the National Pupil Database (NPD), which is owned and managed by the Department 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.

**Transferring data internationally**

Where we transfer personal data to a country or territory outside the European Economic Area, we will do so in accordance with data protection law and only where absolutely necessary (for example when a pupil moves abroad)

**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.

If you would like to make a request please contact our data protection officer.

Parents/carers also have a legal right to access to their child's educational record. To request access, please contact the school.

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 our data protection officer.

**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 our data protection officer.

- 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 our data protection officer:

DPO – Turn it On – Martin Long 01865 597620

## APPENDIX 3: 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' (sometimes called 'fair processing 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, Claycots School, are the 'data controller' for the purposes of data protection law.

Our data protection officer is Turn it On. (see 'Contact us' below).

### 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:

- Contact details
- Date of birth, marital status and gender
- 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 identification documents
- 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 safer recruitment 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 our records retention appendix of this policy.

**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 to share certain information with it, such as safeguarding concerns and exclusions
- Your family or representatives – where it would be necessary to contact them in case of an emergency
- Educators and examining bodies – where it would be necessary to validate qualifications
- Our regulator Ofsted – to allow us to be inspected as an educational provider
- Suppliers and service providers – to enable them to provide the service we have contracted them for, such as payroll
- Financial organisations such as banks – to allow the school to manage its finances effectively. • Our auditors – to allow the school to be proved to be working with integrity
- Health authorities – to allow our pupils and staff to access their services as and where required
- Health and social welfare organisations – to allow our pupils and staff to access their services as and where required
- Professional advisers and consultants– to allow our pupils and staff to access their services as and where required
- Police forces, courts, tribunals – to comply with law enforcement
- Professional bodies
- Educational providers and platforms we consider to enrich the education of the pupils.
- Limited AI platforms vetted and risk-assessed by the school to enhance the school's usual data processing activities.

**Transferring data internationally**

Where we transfer personal data to a country or territory outside the European Economic Area, we will do so in accordance with data protection law and only where absolutely necessary.

**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 our data protection officer.

**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 our data protection officer.

**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 our data protection officer.

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 our data protection officer:

DPO Turn It On, Martin Long 01865 597620

**APPENDIX 4: School Data Retention Rules**

The table below sets out the data retention rules for the school:

| What personal data is stored? | How is it collected? | Retention period |
|---|---|---|
| **(Past/Current/Prospective) Pupil Data** | | |
| Pupil name, address, age, gender, admission date, previous educational establishments | Provided by parent on admission registration forms | DOB + 25yrs |
| Pupil characteristics (age, ethnicity, religion, nationality, first language, national identity) | Provided by parent on admission forms | DOB + 25yrs |
| Pupil medical conditions/doctor details | Provided by parent on admission forms | DOB + 25yrs |
| Pupil special educational needs | Provided by parent/provided by local authority/previous school | DOB + 25yrs |
| Pupil dietary requirements | Provided by parent on admission forms | DOB + 25yrs |
| Pupil meal history | Provided by parent (EYFS/KS1), provided by child (KS2) | 1 term |
| Pupil free school meals/pupil premium/whether they are a looked-after child/service child | Provided by parent on admission forms | DOB + 25yrs |
| Parent/carer/emergency details - name, address contact details, DOB/NI number | Provided by parent on admission registration forms | DOB + 25yrs |
| Photographs of children | Provided by school/third party service | While pupil is at school unless for a specific purpose that requires it is kept for longer (eg. Website photos) |
| Consent forms (photographs, school trips etc) - ARBOR | Provided by parent on ad-hoc basis | DOB + 25yrs |
| Behaviour incidents | Provided by school staff on ad-hoc basis | DOB + 25yrs |
| Attendance information (including exclusions) | Provided by school staff on ad-hoc basis | DOB + 25yrs |
| Accident reports | Provided by school staff on ad-hoc basis | DOB + 25yrs |

| | | |
|---|---|---|
| Pupil admissions applicant information | Provided by SBC | Date of admission/resolution + 1yr |
| Safeguarding details - notes, disclosures, actions and referrals | Reported by staff, recorded discussions with parents | DOB + 25yrs |
| Teacher assessment results | Teacher input/other schools (via CTF/manual input) | DOB + 25yrs |
| Formal assessment results | From LA | DOB + 25yrs |
| Intervention Records | Provided by staff | DOB + 25yrs |

| What personal data is stored? | How is it collected? | Retention period |
|---|---|---|
| **Staff (Applicants/Current/Leavers)** | | |
| Job applicant details (Name, address, contact details, ethnicity/language, qualification details, right to work in the UK details, employment/voluntary details, education/professional institute details, teacher details, personal interest and relationship details, reference details, personal statement) | Job application form, application monitoring form | 6 months from application |
| Interview notes | During interview by interviewing staff | 6 months if not employed, term of employment + 6 yrs If employed |
| Staff details (Name, address, contact details, ethnicity/language, qualification details, right to work details, education/professional institute details, previous employment/voluntary details, teacher details, reference details, training details, statutory checks, contracts, personal interest and relationship details, job application forms) | During employment process/through employment | Term of employment + 6yrs |
| Training details | During employment process/through employment | Term of employment + 6yrs |
| Payroll and staff absence details | During employment process/through employment | Term of employment + 6yrs |
| DBS checks and suitability declaration | By HR admin | Term of employment + 6yrs |

| | | |
|---|---|---|
| Declaration of pecuniary interest | By HR admin | Term of employment + 6yrs |
| Declaration of Health Form | By HR admin | Term of employment + 6yrs |
| Accidents/Near misses at work | From staff | Date of event + 12 yrs |
| Other staff documents (letters, appraisal notes, disciplinary documents) | From senior staff | Term of employment + 6yrs |

| What personal data is stored? | How is it collected? | Retention period |
|---|---|---|
| **Finance** | | |
| Parents/carers payment details | Provided by parents/carers | Deleted as soon as payment is made |
| Supplier details | Provided by staff/suppliers | 7 years |
| Supplier bank details | Provided by staff/suppliers | 7 years |
| Petty cash/expenses claims | Provided by staff | 7 years |
| School fund | Provided by staff/suppliers | 7 years |
| **Governance** | | |
| Governor Details (Name, address, DOB, contact details, training details) | During term of office | Term of governance + 6 yrs |
| Governors register of interests | During term of office | Term of governance + 6 yrs |
| Governors attendance records | During term of office | Term of governance + 6 yrs |
| Governors meeting minutes | During term of office | Permanently |
| Governor applicant details (Name, address, contact details, qualification details, personal interest and relationship details, reference details, personal statement) | During application process | 6 months If unsuccessful |
| Governor Interview notes | During governor interviews | 6 months If unsuccessful |
| **Images/Video** | | |
| CCTV Recordings | CCTV installed around school for security | All footage deleted unless required by law after 30 days |
| Website images | During photography days/ad-hoc | Until pictures are replaced as part of informal website update |
| Internally used images | Ad-hoc | Until pupil leaves school |