EWELL CASTLE SCHOOL
Where Children Thrive

Whole School
(including EYFS)

Data Protection

Table of Contents

Reviewed	Spring 2023
Name of owner/author	SJE/NDH
Approval by	Executive Leadership Team/Governors
Target Audience	Whole School Community/Public
Where available	Website, Staffshared Drive
Review Date	Spring 2024

1 Policy Statement

Ewell Castle 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 provisions of the Data Protection Act 2018 (DPA 2018)

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 GDPR and the 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.

Our Biometric Data Policy meets the requirements of the Protection of Freedoms Act 2012 when referring to our use of biometric data.

Our Closed Circuit Television (CCTV) Policy reflects the ICO's code of practice for the use of surveillance cameras and personal information.

3 Definitions

Term	Definition
Personal data	Any information relating to an identified, or identifiable, individual. This may include the individual's: • Name (including initials) • Identification number • Location data • Online identifier, such as a username It may also include factors specific to the individual's physical, physiological, genetic, mental, economic, cultural or social identity.
Special categories of personal data	Personal data which is more sensitive and so needs more protection, including information about an individual's: • Racial or ethnic origin • Political opinions • Religious or philosophical beliefs • Trade union membership • Genetics • Biometrics (such as fingerprints, retina and iris patterns), where used for identification purposes • Health – physical or mental • Sex life or sexual orientation

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

4 The Data Controller

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.

5.1 Board of Governors

The Board of Governors has overall responsibility for ensuring that our school complies with all relevant data protection obligations. A nominated Governor has specific responsibility for monitoring and overseeing of Compliance.

5.2 The Director of HR & Compliance

The Director of HR & Compliance is responsible for overseeing the implementation of this policy, monitoring our compliance with data protection law and developing related policies and guidelines where applicable.

The Director of HR & Compliance will provide an annual report of the School's activities directly to the governing board and, where relevant, give advice and recommendations on school data protection issues. The Director of HR & Compliance is also the first point of contact for individuals whose data the school processes, and for the ICO.

The Director of HR & Compliance can be contacted by mail at Ewell Castle School, Church Street, Ewell, Surrey KT17 2AW, or by telephone at 020 8393 1413.

5.3 Principal

The Principal acts as the representative of the Data Controller on a day-to-day basis.

5.4 All Staff

Staff are responsible for:

- collecting, storing and processing any personal data in accordance with this policy
- informing the school of any changes to their personal data, such as a change of address
- contacting the Director of HR & Compliance in the following circumstances:
  - with any questions about the operation of this policy, data protection law, retaining personal data or keeping personal data secure
  - if they have any concerns that this policy is not being followed
  - if they are unsure whether or not they have a lawful basis to use personal data in a particular way
  - if they need to rely on or capture consent, draft a privacy notice, deal with data protection rights invoked by an individual, or transfer personal data outside the European Economic Area
  - if there has been a data breach
  - whenever they are engaging in a new activity that may affect the privacy rights of individuals
  - if they need help with any contracts or sharing personal data with third parties.

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

7.1 Lawfulness, Fairness and Transparency

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

- the data needs to be processed so that the School can **fulfil a contract** with the individual, or the individual has asked the School to take specific steps before entering 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 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 GDPR and 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 get parental consent where the pupil is under 12 years old (except for online counselling and preventive services).

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

7.2 Limitation, Minimisation and Accuracy

We will only collect personal data for specified, explicit and legitimate reasons. We will explain these reasons to the individuals when we first collect their data.

If we want to use personal data for reasons other than those given when we first obtained it, we will inform the individuals concerned before we do so, and seek consent where necessary.

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

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

9.1 Subject Access Requests

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

- confirmation that their personal data is being processed
- access to a copy of the data
- the purposes of the data processing
- the categories of personal data concerned
- who the data has been, or will be, shared with
- how long the data will be stored for, or if this isn't possible, the criteria used to determine this period
- the source of the data, if not the individual
- whether any automated decision-making is being applied to their data, and what the significance and consequences of this might be for the individual

Subject access requests must be submitted in writing, either by letter, email or fax to the Principal. 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 Director of HR & Compliance .

9.2 Children and Subject Access Requests

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

Children aged 12 and above are generally regarded to be mature enough to understand their rights and the implications of a subject access request. Therefore, most subject access requests from parents or carers of pupils at our School aged 12 and above may not be granted without the express permission of the pupil. This is based on the School's opinion of the maturity of the child in question, 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 two forms of identification
- may contact the individual via phone to confirm the request was made
- will respond without delay and within one month of receipt of the request
- will provide the information free of charge
- may tell the individual we will comply within three months of receipt of the request, where a request is complex or numerous. We will inform the individual of this within one month, and explain why the extension is necessary

We will not disclose information if it:

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

9.4 Other Data Protection Rights of the Individual

In addition to the right to make a subject access request (see above), and to receive information when we are collecting their data about how we use and process it (see section 7), individuals also have the right to:

- withdraw their consent to processing at any time
- ask us to rectify, erase or restrict processing of their personal data, or object to the processing of it (in certain circumstances)
- prevent use of their personal data for direct marketing
- challenge processing which has been justified on the basis of public interest
- request a copy of agreements under which their personal data is transferred outside 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 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 Principal. If staff receive such a request, they must immediately forward it to the Principal.

10 Photographs and Videos

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

We will obtain written consent from parents/guardians, or pupils aged 16 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/guardian and pupil. Where we require pupil consent, we will clearly explain to the pupil how the photograph and/or video will be used.

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

See our Use of Photographic Images and Photographic Consent Form for more information.

11 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:

- 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
- integrating data protection into internal documents including this policy, any related policies and privacy notices
- regularly training members of staff on data protection law, this policy, any related policies and any other data protection matters; we will also keep a record of attendance
- regularly conducting reviews and audits to test our privacy measures and make sure we are compliant
- maintaining records of our processing activities, including:
    - for the benefit of data subjects, making available the name and contact details of our School and the Director of HR & Compliance 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.

12 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 stored securely when not in use
- 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 must sign it in and out from the school office
- passwords that are at least 7 characters long containing letters and numbers are used to access school computers, laptops and other electronic devices. Staff and pupils are required to change their passwords at regular intervals
- encryption software is used to protect all portable devices and removable media, such as laptops and USB devices
- 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)

13 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.

14 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. 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
- safeguarding information being made available to an unauthorised person
- the theft of a school laptop containing non-encrypted personal data about pupils

15 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.

16 Review and Development

16.1 Procedure

The Principal and Director of HR & Compliance are responsible for monitoring and reviewing this policy.

This policy will be reviewed annually or as events or legislation change requires and shared with the Board of Governors.

16.2 Links with other Policies

This policy should be read in conjunction with the following documents:

Biometric Data Policy
Closed Circuit Television (CCTV) Policy
E-Safety Policy
Acceptable Use Agreements
Privacy Notices
Staff Code of Conduct
Use of Photographic Images and Photographic Consent Form

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 Director of HR & Compliance

The Director of HR & Compliance will investigate the report, and determine whether a breach has occurred. To decide, the
Director of HR & Compliance will consider whether personal data has been accidentally or unlawfully:

- lost
- stolen
- destroyed
- altered
- disclosed or made available where it should not have been
- made available to unauthorised people

The Director of HR & Compliance
will alert the Principal

The Director of HR & Compliance 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 Director of HR & Compliance will assess the potential consequences, based on how serious they are, and how likely they are to happen

The Director of HR & Compliance 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 Director of HR & Compliance will consider whether the breach is likely to negatively affect people's rights and freedoms, and cause them any physical, material or non-material damage (e.g. emotional distress), including through:

- loss of control over their data
- discrimination
- identify theft or fraud
- financial loss
- unauthorised reversal of pseudonymisation (for example, key-coding)
- damage to reputation
- loss of confidentiality
- any other significant economic or social disadvantage to the individual(s) concerned

If it is likely that there will be a risk to people's rights and freedoms, the Director of HR & Compliance must notify the ICO. The Director of HR & Compliance 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 [set out where you keep records of these decisions – for example, on the school's computer system, or on a designated software solution]

Where the ICO must be notified, the Director of HR & Compliance will do this via the 'report a breach' page of the ICO website within 72 hours. As required, the Director of HR & Compliance will set out:

- 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 Director of HR & Compliance
- 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 Director of HR & Compliance 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 Director of HR & Compliance expects to have further information. The Director of HR & Compliance will submit the remaining information as soon as possible.

The Director of HR & Compliance 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 Director of HR & Compliance 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 Director of HR & Compliance
- 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 Director of HR & Compliance 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 Director of HR & Compliance 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 school's computer system.

The Director of HR & Compliance and Principal will meet to review what happened and how it can be stopped from happening again. This meeting will happen as soon as reasonably possible.