Data Protection Policy

Policy first adopted: January 2013

To be reviewed every two years

Reviewed: March 2015

Reviewed: May 2019

Reviewed: March 2021

Reviewed: May 2023

Reviewed May 2025 (Updated July 2025)

Reviewed .....

Introduction

General Statement
Ferndown Upper School fully endorses and adheres to the principles of data protection as outlined in the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018. All staff involved in the collection, processing and disclosure of personal data are aware of their duties and responsibilities under these guidelines. Please also refer to the FOI Publication Scheme for details about what information is held and how it may be accessed.

Enquiries
Information about Ferndown Upper School Data Protection policy can be obtained from the Data Manager. The Data Protection Officer (DPO) is also available for queries.

Fair Obtaining and Processing
Ferndown Upper School undertakes to obtain and process data fairly and lawfully.

Terms
Processing - Obtaining, recording or holding the information or data or carrying out a set of operations on the information or data.
Data subject - means an individual who is the subject of personal data or the person to whom the data relates.
Personal data - means data which relates to a living individual who can be identified. Addresses and telephone numbers are examples.
Parent - *refers* to the meaning given in the Education Act 1996, and includes any person who has parental responsibility for a child.

Lawful Basis and Registered Purposes
Ferndown Upper School processes personal data primarily under the lawful basis of "public task" (Article 6(1)(e), UK GDPR), necessary for performing its official functions. Consent is sought where required, e.g., for biometric data. Data is processed only for the purposes registered with the Information Commissioner's Office (ICO), and not used for any other purpose without the data subject's consent. Explanation of any codes and categories is available from the School Business Manager who is the person nominated to deal with data protection issues.

Data Integrity
Ferndown Upper School undertakes to ensure that data integrity is achieved by the following methods:

Data Accuracy
Data will be as accurate and up-to-date as is reasonably possible. If a data subject informs the school of a change of circumstances their computer record will be updated as soon as is practicable. A printout of their data record will be provided to any data subjects every twelve months so they can check its accuracy and make any amendments. Where a subject challenges the accuracy of their data, Ferndown Upper School will update the data as soon as is practicable. In cases of dispute, we will attempt to resolve the issue informally, but if this proves impossible, disputes will be referred to the Headteacher, for their judgement. If the dispute cannot be resolved at this stage, the matter will be passed to a Panel of three school Governors, please see the school's Complaints Policy.

Data Retention

Data held about individuals will not be kept for longer than necessary for the purposes registered. It is the duty of the Data Manager to ensure that obsolete data are properly erased. The Data Protection Officer (DPO) is also available for queries

Subject Access

The Data Protection Acts extend to all data subjects a right of access to their own personal data. In order to ensure that people receive only information about themselves it is essential that a formal system of requests is in place. Where a request for subject access is received from a pupil, the school's policy is that:

- Requests from pupils will be processed as any subject access request as outlined below, unless it is clear that the pupil does not understand the nature of the request.

- Requests from pupils who do not appear to understand the nature of the request will be referred to their parents or carers.

- Requests from parents in respect of their own child will be processed as requests made on behalf of the data subject (the child) with the child's permission and the copy will be available to be collected from Reception on a date and time agreed.

Processing Subject Access Requests

Requests for access must be made in writing.
Provided that there is sufficient information to process the request, an entry will be made in the Subject Access Log, A Subject Access Log records the request date, requester details, data type and expected response date. The school will respond within one calendar month of receiving sufficient information.

Authorised Disclosures

Ferndown Upper School will, in general, only disclose data about individuals with their consent. However, there are circumstances under which the school's authorised officer may need to disclose data without explicit consent for that occasion.

These circumstances are strictly limited to:

- Pupil data disclosed to authorised recipients related to education and administration necessary for the school to perform its statutory duties and obligations.

- Pupil data shared between other schools and outside agencies for the purposes of coordinating services between schools.

- Pupil data disclosed to authorised recipients in respect of their child's health, safety and welfare. Safeguarding information will be shared or withheld depending on the potential impact on student safety.

- Pupil data disclosed to parents in respect of their child's progress, achievements, attendance, attitude or general demeanour within the vicinity of the school.

- Staff data disclosed to relevant authorities e.g., in respect of payroll and administrative matters.

- Unavoidable disclosures, for example to an engineer during maintenance of the computer system. In such circumstances the engineer would be required to sign a form promising not to disclose the data outside the school.

- Only authorised and trained staff are allowed to make external disclosures of personal data. Data used within the school by administrative staff, teachers and welfare officers will only be made available where the person requesting the information is a professional legitimately working within the school who need to know the information in order to do their work. We will not disclose anything on pupils' records which would be likely to cause serious harm to their physical or mental health or that of anyone else – including anything where suggests that they are, or have been, either the subject of or at risk of child abuse.

A **"legal disclosure"** is the release of personal information from the computer to someone who requires the information to do his or her job within or for the organisation, provided that the purpose of that information has been registered.

An **"illegal disclosure"** is the release of information to someone who does not need it, or has no right to it, or one which falls outside the organisation's registered purposes.

Data and Computer Security
Ferndown Upper School undertakes to ensure security of personal data by the following general methods (precise details cannot be revealed):

Physical Security

Appropriate building security measures are in place, such as alarms, window bars, deadlocks and computer hardware cable locks. Only authorised persons are allowed in the computer server areas. Disks, tapes and printouts are locked away securely when not in use. Visitors to the school are required to sign in and out, to wear identification badges whilst in the school and are, where appropriate, accompanied.

Logical Security
Security software is installed on all systems containing personal data. Access is restricted through multi-factor authentication, encrypted storage solutions, and strict user permissions. Password policies are enforced and reviewed. Cloud platforms are monitored and data is backed up routinely.

Backups and Retention: The school's digital systems are backed up daily and weekly to secure on-site storage devices with built-in redundancy to ensure continuity in the event of failure. Weekly backups are stored in a way that isolates them from the network to protect against cyber threats. Cloud-based data such as emails, documents, and learning platforms is backed up separately using an encrypted online backup service. Management Information System (MIS) data is also backed up externally. Backup data is stored securely and retained through a controlled overwrite cycle.

1 day retention to one of the backup devices
7 day retention to the air gapped backup device

Windows Server Backups

1 day retention

Cloud to Cloud Backups
18 months

Procedural Security
In order to be given authorised access to the computer, staff will have to undergo checks and will sign a confidentiality agreement. All staff are trained in their Data Protection obligations and their knowledge updated as necessary. Computer printouts as well as source documents are shredded before disposal. Overall security policy for data is determined by the Headteacher and Governing Body and is monitored and reviewed regularly.

Any queries or concerns about security of data in the school should in the first instance be referred to the Data Manager.

Individual members of staff can be personally liable in law under the terms of the Data Protection Acts. They may also be subject to claims for damages from persons who believe that they have been harmed as a result of inaccuracy, unauthorised use or disclosure of their data. A deliberate breach of this Data Protection Policy will be treated as a disciplinary matter.

Use of Artificial Intelligence (AI)

Ferndown Upper School acknowledges the growing use of Artificial Intelligence (AI) technologies in education and administration. Where AI tools are used in data processing or decision-making, the school will ensure that:

AI systems used must be vetted, risk assessed, and approved by the Data Protection Officer (DPO) and/or Headteacher before use. This applies to administrative systems, teaching support tools, or any other AI-driven platforms.

- Parental and pupil data will not be shared with third-party AI platforms.

- Personal data processed by AI tools is subject to the same standards of protection, minimisation, and purpose limitation as all other data.

- Staff are aware of the limitations and risks of using AI tools, including bias, data accuracy, and security vulnerabilities.

- AI systems do not make fully automated decisions that have a legal or similarly significant effect on individuals, unless a lawful basis is established and safeguards are in place.

- All processing complies with the UK GDPR principles, particularly regarding transparency, fairness, and accountability.

Data Breach Reporting
In the event of a personal data breach, Ferndown Upper School will assess the risk to individuals and report any notifiable breach to the Information Commissioner's Office (ICO) within 72 hours. Affected individuals

will be informed without undue delay. All incidents are recorded, reviewed, and actioned by the Data Protection Officer (DPO).

Biometrics

In accordance with the Protection of Freedoms Act 2012 and the Data Protection Act 2018 (DPA) below sets how such data will be used by Ferndown Upper School.

Biometric information is information about a person's physical or behavioural characteristics that can be used to identify them, for example, information from their fingerprint. It is defined in the Data Protection Act as "personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of an individual, which allows or confirms the unique identification of that individual, such as facial images or dactyloscopic data."

Biometric information may be used for a range of applications and services including but not limited to access and exit for the school's premises, access to services such as library or paying for meals in the canteen, attendance records and computer services.

Currently the school only uses fingerprint information as part of an automated biometric recognition system. This system takes measurements of a person's fingerprints and converts these measurements into a template to be stored on the system. A full image of the fingerprint is not stored. The template (i.e. measurements taking from the fingerprint) is what will be used to permit access to the service.

The use of the biometric system is by written consent and if consent is not available the school will always ensure there is another means of providing access to the application or service.

A student may object or refuse to participate (or to continue to participate) in activities that involve the processing of their biometric data, and this objection or refusal overrides any parental consent to the processing.

If consent is refused the school will ensure that the student's biometric data are not taken/used as part of a biometric recognition system or if taken destroyed following withdrawal of consent.

Further information and guidance "Protection of children's biometric information in schools Guidance for schools, sixth-form colleges, 16 to 19 academies and further education institutions wishing to use automated biometric recognition systems." https://www.gov.uk/government/publications/protection-of-biometric-information-of-children-in-school