Foreland Fields School

Data Protection Policy

Governing Body Approval and Categories

Date of Last Review / Scrutiny	18th November 2025
Date (Month / Year) of Next Review /Scrutiny	November 2026
Date Policy was Ratified	3rd December 2025
Category of the Policy	GDPR
Named Lead for Writing the Policy	School Business Manager in conjunction with School Data Protection Officer
Named Governor for Scrutiny	Chair of Governors / Governor with Responsibility for Safeguarding
Approval Body	Full Governing Body
Display on Main Web Site	Yes
NOTE: IF THIS POLICY HAS BEEN SCRUTINISED BY A DIFFERENT LEAD GOVERNOR OR BEEN RATIFIED BY A DIFFERENT GOVERNING TEAM PLEASE STATE WHICH TEAM	
Signed – Chair of Governors	Date 3-12-25

United Nations Convention on the Rights of the Child

Foreland Fields School is a Rights Respecting School thereby this policy ensures that the following rights are acknowledged:

Article 13 (freedom of expression)
Every child must be free to express their thoughts and opinions and to access all kinds of information, as long as it is within the law.

Article 16 (right to privacy)
Every child has the right to privacy. The law should protect the child's private, family and home life, including protecting children from unlawful attacks that harm their reputation.

Article 36 (other forms of exploitation)
Governments must protect children from all other forms of exploitation, for example the exploitation of children for political activities, by the media or for medical research.

Foreland Fields School
Data Protection Policy

Links with Other Policies

This data protection policy is linked to our:

- Freedom of information publication scheme
- Online Safety Policy
- Acceptable Use of Technology Policies
- Child Protection Policy
- Waste Management Policy
- Mental Capacity Policy
- Image Use Policy
- Whistleblowing Policy

Introduction

General Data Protection Regulation (GDPR) and the Data Protection Act 2018(DPA) is the law that protects personal privacy and upholds individuals' rights. It applies to anyone who handles or has access to people's personal data.

This policy is intended to ensure that personal information is dealt with properly and securely and in accordance with the legislation. It will apply to personal information regardless of the way it is used, recorded and stored and whether it is held in paper files or electronically.

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 data protection legislation.

This policy applies to all personal data, regardless of the way it is used, recorded and stored and whether it is held in paper or electronic format.

Legislation and Guidance

The school as the Data Controller will comply with its obligations under the GDPR and DPA. The school is committed to being concise, clear and transparent about how it obtains and will ensure data subjects are aware of their rights under the legislation.

All staff must have a general understanding of the law and understand how it may affect their decisions in order to make an informed judgement about how information is gathered, used and ultimately deleted. All staff must read and understand this policy.

This policy meets the requirements of all data protection legislation. It is based on guidance published by the Information Commissioner's Office (ICO).

It also reflects the ICO guidance for the use of surveillance cameras and personal information. (https://icosearch.ico.org.uk/s/search.html?collection=ico-meta&query=guide+use+of+cameras&profile=_default)

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.

Scope of the Policy

Personal data is any information that relates to an identified or identifiable living individual who can be identified directly or indirectly from the information. The information includes factor specific to the physical, physiological, genetic, mental, economic, cultural or social identity of living individual. This includes any expression of opinion about an individual and intentions towards an individual. Under GDPR personal information also includes an identifier such as name, an identification number, location data or an online identifier.
The School collects a large amount of personal data every year including: pupil records, staff records, names and addresses of those requesting prospectuses, examination marks, references, fee collection as well as the many different types of research data used by the school. In addition, it may be required by law to collect and use certain types of information to comply with statutory obligations of Local Authority (LA's), government agencies and other bodies.

Definitions

TERM	DEFINITION
Personal data	Any information relating to an identified, or identifiable, living 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.

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 with the ICO and has paid its data protection fee to the ICO, as legally required.

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

Foreland Field School's 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) will work with the school to ensure compliance with obligations under the General Data Protection Regulation and any relevant UK legislation.
The DPO will provide an annual report of their activities directly to the Governing Body and, where relevant, report 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 is Alan Martin and is contactable via email: alan@dataprotectionadviceltd.co.uk

Headteacher – Senior Information Risk Owner (SIRO)
The SIRO acts as the representative of the data controller on a day-to-day basis. The SIRO provides board-level accountability and greater assurance that information risks are addressed.

Information Champion – School Business Manager
Information Champions play a key role in ensuring that Foreland Fields School maintains an effective framework for managing information, enabling business needs to be met within an agile and flexible environment and allowing us to work closely with partners, exchanging information legally, safely and securely.

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 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.

Data Protection Principles

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

1. Processed **lawfully, fairly** and in a **transparent** manner.
2. Collected for specified, explicit and legitimate purposes. **(Purpose limitation)**
3. Adequate, relevant and limited to what is necessary to fulfil the purposes for which it is processed**. (data minimization)**
4. Accurate and, where necessary, kept up to date. **(Accuracy)**
5. 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. **(Storage Limitation)**
6. Appropriate technical and organisational measures shall be taken to safeguard the rights and freedoms of the data subjects, to ensure that personal information processed in a manner that ensures appropriate security of the personal data and protects against unauthorized or unlawful processing of personal data and against accidental loss or destruction of or damage to personal data. **(Integrity and confidentiality).**

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

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:

- 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.** Agreement will be obtained through a clear statement or positive action to the processing. Consent will be affirmative action so silence, pre-ticked boxes or inactivity will not be accepted. If consent is given it will be separate from other matters. The data subject will be easily able to withdraw consent to processing at any time and withdrawal will be promptly honoured.
  Consent may need to be reviewed if personal data is intended to be processed for a different and incompatible purpose which was not disclosed when the data subject first gave consent

For Information about both the purposes of the processing and the lawful basis, please refer to the school's privacy notice(s) for greater detail.

For special categories of personal data, we will also meet one 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. (Explained in the school's privacy notice)**
- The data needs to be processed to perform or exercise obligations or rights in relation to **employment, social security or social protection law.**
- The processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade-union aim
- The processing is necessary for purposes of preventative or occupational medicine, for the assessment of the working capacity of the employee, the provision of social care and the management of social care systems or services

- 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.

Sensitive personal information will not be processed until an assessment has been made of the proposed processing as to whether it complies with the criteria above and the individual has been informed (by way of a privacy notice or consent) of the nature of the processing, the purposes for which it is being carried out and the legal basis for it.

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.
The school privacy notice includes types of sensitive personal information being processed and the conditions which apply

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.
Staff will ensure that data subjects are informed of the period for which data is stored and how that period is determined in any applicable Privacy Notice.
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 to ensure personal data is deleted after a reasonable time for the purpose for which it was being held, unless a law requires such data to be kept for a minimum time.
Staff must take all reasonable steps to destroy or delete all personal data that is held in its systems when it is no longer required in accordance with the Schedule. This includes requiring third parties to delete such data where applicable.

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:

- 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 which can provide sufficient guarantees that they comply with 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.
- The organisation may only act on the written instructions of the school
- the organisation will delete or return all personal information to the school as requested at the end of the contract
- The organisation will submit to audits and inspections, provide the school with whatever information it needs to ensure that they are both meeting their data protection obligations, and tell the school immediately if it does something infringing data protection law.

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 data protection law.

Subject Access Requests and other Rights of Individuals

There are two distinct rights of access to personal information held by schools.

- **Under the GDPR and the Data Protection Act 2018** an individual (e.g. pupil, parent or member of staff) has a right to request access to their own personal information. In certain circumstances requests may be made by a parent on behalf of their child (see explanation below).
- **The Education (Pupil Information) (England) Regulations 2005** gives parents the right of access to curricular and educational records relating to their child.

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.

Processing a Request

Requests for personal information must be made in writing and addressed to the Headteacher. The following information will be required

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

If the initial request does not clearly identify the information required, then clarification will be sought.

The identity of the requestor must be verified before the disclosure of any personal information, and checks will also be carried out regarding proof of relationship to the child.

Evidence of identity can be established by requesting production of the following (this list is not exhaustive) prior to proceeding with the access rights:

- passport
- driving licence
- utility bills with the current address
- Birth / Marriage certificate
- P45/P60
- Credit Card or Mortgage statement
- Parental Responsibility

In addition to a copy of their personal data, you also have to provide individuals with the following information:

- the purposes for processing their data;
- the categories of personal data concerned;
- the recipients or categories of recipient you disclose the personal data to;
- your retention period for storing the personal data or, where this is not possible, your criteria for determining how long you will store it;
- the existence of their 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;
- information about the source of the data, where it was not obtained directly from the individual;
- the existence of automated decision-making (including profiling); and
- the safeguards you provide if you transfer personal data to a third country or international organisation.

Much of this information will already be included in the school's privacy notice.

Information can be viewed at the school with a member of staff on hand to help and explain matters if requested or provided at a face to face handover.
The views of the applicant should be considered when considering the method of delivery. If the applicant has asked for the information to be posted then special next day delivery or recorded delivery postal service must be used.

If staff receive a subject access request in any form they must immediately forward it to the Information Champion.

Foreland Field School follows a recommended Subject Access Request (SAR) appropriately and within the required timescales, based on the guidance in the IRMS School Tool kit

https://irms.org.uk/page/SchoolsToolkit

Children and Subject Access Requests

Children have the same rights of access to their own personal information as adults, and the same rights of privacy. There is no minimum age in English law, however current practice accepts that, provided a child is mature enough to understand their rights, a child of, or over the age of 13 years shall be considered capable of giving consent. This does not rule out receipt of a valid request from a child of a younger age, as each request should be considered on its merits on an individual basis.

When a subject access request is received from a child it will need to be judged whether the child has the capacity to understand the implications of their request and of the information provided as a result of that request. If the child does understand then their request will be dealt with in the same way as that of an adult. Within Special Schools however, this is not a rule and a pupil's ability to understand their rights will always be judged on a case-by-case basis.

If a parent or legal guardian makes a request on behalf of a child age 13 and over the request will only be complied with when assurances are received that the child has authorised the request and that their consent was not obtained under duress or on the basis of misleading information. If the child does not understand, then a request from a parent or legal guardian for the child's information will only be complied with when assurances are received that they are acting in the best interests of the child.

Responding to Subject Access Requests

The response time for compliance with a subject access request is **one month** following date of receipt. The timeframe does not begin until the school has received all the information necessary to comply with the request i.e.

- 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.

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 consider whether the request is repetitive in nature when making this decision.

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.

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, 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 if it is no longer necessary for the purpose for which it was originally collected/processed, or if there are no overriding legitimate grounds for the processing ('the right to be forgotten')
- To request a copy of an agreement under which personal data is transferred outside of the EEA
- Prevent use of their personal data for direct marketing.
- Object to processing which has been justified on the basis of public interest, official authority or legitimate interests.
- 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).
- To obtain confirmation that personal information is being processed and to obtain access to it and certain other information, by making a subject access request

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 Information Champion who will contact the DPO.

Parental Requests to see Educational Records

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.

CCTV

Foreland Fields School use CCTV in various locations around the school site to ensure it remains safe. We will adhere to the ICO's https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/cctv-and-video-surveillance/ for the use of CCTV.

Foreland Fields School does 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 Karen Glover, School Business Manager.

Use of GPS Tracking

Staff/parents/carers should refer to and follow the appropriate sections in the school online safety policy and the procedure for supporting pupils at risk of absconsion – use of GPS trackers. The use of Airtags has been vetted and assessed by the school DPO. The data collected by Airtags is encrypted and sent to a school iPhone.

Photographs and Videos

As part of our school activities, we may take photographs and record images of individuals within our school.
These are used for assessment and recording purposes, e.g. in the Progress Files seen at EHCP review meeting. Where photos/videos are required as part of curricular records and assessments our legal basis is public task, as the photos or videos are necessary to fulfil our function as a school.

We will obtain written consent from parents/carers for photographs and videos to be taken of their child for marketing and promotional materials. We will clearly explain how the photograph and/or video will be used to both the parent/carer and 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. This is to protect all members of the school community.

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

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.
- Special school events.
- Online applications – see below

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.

Many images taken and held are now electronic. Use of video and photos to support assessment of pupil progress, feedback to pupils and parents and parent feedback to the school is now an integral part of the schools working practice as part of its public duty. The school uses several online services / apps to support Teaching and Learning, Assessment and communication with Parents/Carers. These include; ClassDojo. Seesaw, Microsoft teams, Google Hangouts, YouTube, Tapestry, Evidence for learning, Iris. Refer to the Online safety policy for full detail on how images are managed and kept safe in these contexts. For all Online services the following steps are taken; Privacy notices updated (as well as directly informing parents and stake holders), data processor contracts added to Information audit, legal basis (public duty and occasionally consent) established, Data protection / Privacy impact assessments (DPIA/PIA) made, Information audits and records management processes updated. Staff, parents and stakeholders (as appropriate) informed and /or consent gained. Clear, easy to follow training and notification communicated to all parties as appropriate.

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.
- 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 European Economic Area (EEA), where different data protection laws will 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 EEA and the safeguards for those, retention periods and how we are keeping the data secure.

Automated Decision Making

Where the school carries out automated decision making (including profiling) it must meet all the principles and have a lawful basis for the processing. Explicit consent will usually be required for automated decision making (unless it is authorised by law or it is necessary for the performance of or entering into a contract).
Additional safeguards and restrictions apply in the case of solely automated decision-making, including profiling. The School will as soon as reasonably possible notify the data subject in writing that a decision has been taken based on solely automated processing and that the data subject may request the school to reconsider or take a new decision. If such a request is received staff must contact the DPO as the school must reply within 21 days.

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.
- 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. Additionally, all devices containing personal information (or which can be used to access it) from the school's premises unless appropriate security measures are in place (such as pseudonymisation, encryption or password protection) to secure the information and the device
- Passwords that are at least 8 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.
- All staff are responsible for keeping information secure in accordance with the legislation and must follow their school's acceptable usage policy.
- The school will develop, implement and maintain safeguards appropriate to its size, scope and business, its available resources, the amount of personal data that it owns or maintains on behalf of others and identified risks (including use of encryption and pseudonymisation where applicable). It will regularly evaluate and test the effectiveness of those safeguards to ensure security of processing.

Staff must comply with and not attempt to circumvent the administrative, physical and technical safeguards the school has implemented and maintains in accordance with the GDPR and DPA.

Where the school uses external organisations to process personal information on its behalf, additional security arrangements need to be implemented in contracts with those organisations to safeguard the security of personal information. Contracts with external organisations must provide that:

- the organisation will only act on the written instructions of the school
- those processing data are subject to the duty of confidence
- appropriate measures are taken to ensure the security of processing
- sub-contractors are only engaged with the prior consent of the school and under a written contract
- the organisation will assist the school in providing subject access and allowing individuals to exercise their rights in relation to data protection
- the organisation will delete or return all personal information to the school as requested at the end of the contract
- the organisation will submit to audits and inspections, provide the school with whatever information it needs to ensure that they are both meeting their data protection obligations, and tell the school immediately if it does something infringing data protection law.
- keep personal information secure (e.g. by complying with rules on access to premises, computer access, password protection and secure file storage and destruction in accordance with the school's policies).
- not store personal information on local drives or on personal devices that are used for work purposes.

Before any new agreement involving the processing of personal information by an external organisation is entered into, or an existing agreement is altered, the relevant staff must seek approval from the DPO.

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.
Staff should adhere to the KCC Information Management Toolkit for Schools on KELSI with reference to the Record Retention Schedule, available at the following link:
https://www.kelsi.org.uk/school-management/data-and-reporting/access-to-information/records-management
Foreland Fields School will shred paper-based records, and overwrite or delete electronic files. We also use a third party to safely dispose of records on the school's behalf. We require the third party to provide sufficient guarantees that it complies with data protection law.

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 for Reporting or Handling a Security Incident.
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 pupil 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.
- Unauthorised access to or use of personal information either by a member of staff or third party
- Loss of data resulting from an equipment or systems (including hardware or software) failure
- Human error, such as accidental deletion or alteration of data
- Unforeseen circumstances, such as a fire or flood
- Deliberate attacks on IT systems, such as hacking, viruses or phishing scams
- Blagging offences where information is obtained by deceiving the organisation which holds it

Staff should ensure they inform their line manager/DPO/Head teacher immediately that a data breach is discovered and make all reasonable efforts to recover the information, following the school's agreed breach reporting process.

Data Protection Impact Assessments (DPIA)

All data controllers are required to implement 'Privacy by Design' when processing personal data.

This means the School processes must embed privacy considerations and incorporate appropriate technical and organisational measures (like pseudonymisation) in an effective manner to ensure compliance with data privacy principles.

Where processing is likely to result in high risk to an individual's data protection rights (for example where a new technology is being implemented) a DPIA must be carried out to assess:

- whether the processing is necessary and proportionate in relation to its purpose
- the risks to individuals
- what measures can be put in place to address those risks and protect personal information.

Staff should adhere to the Data Protection Toolkit for Schools from the DfE with reference to the DPIA template.

When carrying out a DPIA, staff should seek the advice of the DPO for support and guidance and once complete, refer the finalised document to the DPO for sign off.

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.

Monitoring Arrangements

The DPO is responsible for monitoring and reviewing this policy.

This policy will be reviewed Annually and shared with the Full Governing Board.

Additional Information

Why, Must and Do Procedures – Data Protection

Must, Why and Do Procedures - Data Protection

General rules in complying with Data Protection law

The points are numbered. The numbering corresponds to explanations of 'why?' and 'how?' for each point further down the page.

What must I do?

1. ***MUST***: All employees must **comply** with the requirements of Data Protection Law and Article 8 of the Human Rights Act when processing the personal data of living individuals
2. ***MUST***: Where personal data is used we must make sure that the data subjects have access to a complete and current **Privacy Notice.**
3. ***MUST:*** We must formally **assess** the risk to privacy rights introduced by any new (or change to an existing) system or process which processes personal data
4. ***MUST***: We must process only the **minimum** amount of personal data necessary to deliver services.
5. ***MUST***: All employees who record **opinions** or intentions about service users must do so carefully and professionally
6. ***MUST***: We must take reasonable steps to ensure the personal data we hold is **accurate**, up to date and not misleading.
7. ***MUST***: We must rely on **consent** as a condition for processing personal data only if there is no relevant legal power or other condition
8. ***MUST***: Consent must be obtained if personal data is to be used for **promoting or marketing** goods and services.
9. ***MUST***: We must ensure that the personal data we process is reviewed and **destroyed** when it is no longer necessary.
10. ***MUST***: If we receive a **request** from a member of the public or colleagues asking to access their personal data, we must handle it as a Subject Access Request

https://www.kelsi.org.uk/__data/assets/pdf_file/0008/94751/Information-Management-Toolkit-Early-Years-Provision.pdf

https://ico.org.uk