Data Protection Policy

Reviewed 17.09.2024

Next Review Sept 2025

Fairfields School

Approved by Governors 14.10.24

1. Aims

Fairfields School is committed to the protection of all personal and sensitive data for which it holds responsibility as the Data Controller, the handling of such data in line with the data protection principles (see below), the General Data Protection Regulation (EU) 2016/679 (GDPR) and the Data Protection Act 2018 (DPA 2018).

2. Legislation and guidance

This policy meets the requirements of the GDPR and the DPA 2018. It is based on guidance published by the Information Commissioner's Office (ICO) on the UK GDPR.

It meets the requirements of the Protection of Freedoms Act 2012 when referring to our use of biometric data.

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.

Data protection legislation shall be monitored and implemented to remain compliant with all requirements.

Article 6 Lawfulness of processing

Processing is necessary for the performance of a task carried out in the **public interest** or in the exercise of official authority vested in the controller;

Article 9 Processing of special categories of personal data

1. Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited.

2. Paragraph 1 shall not apply if one of the following applies:

1. (a) the data subject has given explicit consent to the processing of those personal data for one or more specified purposes, except where Union or Member State law provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject;

The requirements of this policy are mandatory for all staff employed by us and any third party contracted to provide services.

If personal information meets the above criteria, then individuals who have personal information held by us will be made aware of the personal information and the criteria for holding the information in the 'Information Audit' document.

3. 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
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.

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 will renew its data protection fee to the ICO annually, as 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 Data Controller

The data controller is the person who determines the purposes for which and the manner in which any personal data are processed. The governing board has overall responsibility for ensuring that our school complies with all relevant data protection obligations and is therefore the data controller. The headteacher acts as the representative of the data controller on a day-to-day basis. The Headteacher may delegate data controller duties as necessary.

5.2 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 board and, where relevant, report to the board their advice and recommendations on school data protection issues.

The DPO is also the first point of contact for individuals whose data the school processes, and for the ICO.

The DPO monitors internal compliance and informs and advises the school about their data protection obligations and acts as a contract point for data subjects and the supervisory authority. The DPO is independent, an expert in data protection, adequately resourced and reports to the highest management level.

Our DPO is: **Ruth Hawker**, Plumsun Ltd, Almshouses, Great Brington, Northampton, NN7 4JJ

Tel: **08458622684**

5.3 All staff

Staff are responsible for treating all personal information in a confidential manner and follow the guidelines set out in this document. This includes:

- 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
    - If they need help with any contracts or sharing personal data with third parties

5.4 External Parties

Any data processors, processing data on behalf of the school (external organisations) will confirm that they are achieving their obligations under the GDPR regulations and are registered with the ICO.

6. Data protection principles

Under the UK GDPR, the data protection principles set out the main responsibilities for organisations.

Article 5 of the UK GDPR requires that personal data shall be:

(a) Processed lawfully, fairly and in a transparent manner in relation to individuals;

(b) Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposed in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes.;

(c) Adequate, relevant and limited to what is necessary to fulfil the purposes for which it is processed;

(d) Accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are3 inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;

(e) Kept in a form which permits information of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the UK GDPR in order to safeguard the rights and freedoms of individuals; and

(f) Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisation measures.

Article 5(2) requires that "the controller shall be responsible for, and be able to demonstrate, compliance with the principles." Notifications shall be in accordance with ICO guidance and, where relevant, be written in a form understandable by those defined as "children" under the legislation.

We will ask for consent to hold and process personal information if there is no lawful basis for doing so.

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. For example the data needs to be processed so that:

- the school can **fulfil a contract** with the individual
- the school can **comply with a legal obligation**
- the **vital interests** of the individual or another person are ensured i.e. to protect someone's life
- the school, as a public authority, can **perform a task in the public interest or exercise its official authority**
- the **legitimate interests** of the school (where the processing is not for any tasks the school performs as a public authority) or a third party, provided the individual's rights and freedoms are not overridden
- The individual (or their parent/carer when appropriate in the case of a pupil) has freely given clear **consent**

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

- The data needs to be processed for **public health reasons**, and the processing is done by, or under the direction of, a health professional or by any other person obliged to confidentiality under law
- The data needs to be processed for **archiving purposes**, scientific or historical research purposes, or statistical purposes, and the processing is in the public interest

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

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

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

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

7.2 Limitation, minimisation and accuracy

- We will only collect personal data for specified, explicit and legitimate reasons. We will explain these reasons to the individuals when we first collect their data.
- If we want to use personal data for reasons other than those given when we first obtained it, we will inform the individuals concerned before we do so, and seek consent where necessary.
- Staff must only process personal data where it is necessary in order to do their jobs.
- We will keep data accurate and, where necessary, up-to-date. Inaccurate data will be rectified or erased when appropriate.
- In addition, when staff no longer need the personal data they hold, they must ensure it is deleted or anonymised. This will be done in accordance with the school's record retention schedule, in line with the Information and Records Management Society's toolkit for schools.

8. Sharing of Information with Third Parties

There may be circumstances where the school is required either by law or in the best interests of students or staff to pass on information to external authorities (e.g. Ofsted, Local Authority). These authorities must adhere to data protection law and have their own policies relating to the protection of any data that they receive or collect.

Personal data about pupils will not be disclosed to third parties without the consent of the parent or carer, unless it is obliged by law or in the best interest of the child.

Examples of data that may be disclosed to third parties without the need for consent:

- Pupil transferring to another school – their academic record and data regarding health and welfare will be shared with the new school
- Under health legislation, the school may pass on information to health authorities regarding the health of the pupil in the interest of public health.
- A criminal investigation is being carried out, we may have to forward information to the police.
- In order to protect the welfare of pupils, it may be necessary to share personal data with social workers

The intention to share data relating to individuals to an external organization shall be clearly defined within notifications and details of the basis for sharing given. These details are provided in the Information Audit document on the school Sharepoint. Data will be shared with external parties in circumstances where it is a legal requirement to provide such information, or where it is for the purpose of pupil provision, such as school meals or curriculum.

Any proposed change to the processing of an individual's data shall be notified to them. Under no circumstances will the school disclose information or data:

- That would cause serious harm to the child or anyone else's physical or mental health or condition.
- Indicating that the child is or has been subject to child abuse or may be at risk of it, where the disclosure would not be in the best interest of the child
- That would allow another person to be identified or identifies another person as the source, unless the person is an employee of the school or a local authority or has given consent, or it is reasonable in the circumstances to disclose the information without consent the exemption from disclosure does not apply if the information can be edited so that the person's name or identifying details are removed
- Any situation where it would not be in the best interest of the child.

Where we transfer personal data internationally, we will do so in accordance with data protection law.

9. Subject access requests and rights of individuals

9.1 Subject access requests

All individuals whose data is held by the school, has a legal right to request access to such data or information. A child may make a subject access request themselves, specified under GDPR guidance. The school shall respond to such requests in one month. This includes:

- Confirmation that their personal data is being processed
- Access to a copy of the data
- The purposes of the data processing
- The categories of personal data concerned
- Who the data has been, or will be, shared with
- How long the data will be stored for, or if this isn't possible, the criteria used to determine this period
- Where relevant, the existence of the right to request rectification, erasure or restriction, or to object to such processing
- The right to lodge a complaint with the ICO or another supervisory authority
- The source of the data, if not the individual
- Whether any automated decision-making is being applied to their data, and what the significance and consequences of this might be for the individual
- The safeguards provided if the data is being transferred internationally

Subject access requests should be made in writing to the Headteacher and include:

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

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

When responding to requests, we:

- May ask the individual to provide 2 forms of identification
- May contact the individual via phone to confirm the request was made
- 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

In line with safeguarding and GDPR obligations, some personal information may be redacted for reasons such as:

- Information that might cause serious harm to the physical or mental health of the pupil or another person
- Information requested that would not be in the best interest of the child
- Information containing personal information about more than one individual

The DPO will independently advise on any requests. No charge will be applied. If we refuse a request, we will tell the individual why, and tell them they have the right to appeal to the ICO or they can seek to enforce their subject access right through the courts.

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 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.

9.4 Other data protection rights of the individual

Individuals have the right to:

- Be informed about what data is being held (Information Audit document)
- Be informed about how and why the data is being processed (Information Audit document)
- The right to access any data that is being held (Subject Access Request)
- The right to request that any data is erased.
- The right to restrict processing
- The right to data portability if the data is held by automatic means
- The right to object to the way the data is held or processed
- The right not to be subject to automated decision-making

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 DPO.

9.5 Right to be Forgotten

Where any personal data is no longer required for its original purpose, an individual can demand that the processing is stopped, and all their personal data is erased by us including any data held by contracted processors.

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.

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.

11. Photographs and videos

Due to carrying out our public duty, the school does not ask for consent from parents when making decisions to use pictures and social media to promote educational progression of pupils for parents. It also forms evidence of educational attainment for Ofsted and the DFE. However, the school does encourage parents to raise any safeguarding concerns to the school, and staff will respond in a proactive manner.

Photographs and social media are used to ensure that when on visits, evidence of pupils educational attainment is recorded. This is for educational use only and informs the parents of the students progression. The school takes safeguarding concerns seriously, and so a statement reflects this, should there be any concerns regarding their pupils.

The Information Audit and Privacy Notice provides information regarding the use of photographs used on the website and in electronic newsletters. Photographs and videos are only captured for educational purposes and are not shared with external parties

12. Protection Impact Statements

We will evidence the thought and decision-making process about data protection when designing any processes in school which involve personal data. A Data Protection Impact Statement (DPIA) is needed when it is likely to result in potentially high risk:

- New technology is being deployed
- A profiling operation is likely to significantly affect individuals
- There is processing on a large scale of the special categories o data (special categories as specified in UK GDPR guidance).

13. 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:

The following guidelines are in place for staff in order to reduce the risk of personal data being compromised:

- Paper copies of data or personal information should not be take off the school site unless the data controller has provided permission to do so (e.g. emergency information for educational visits). The data should not be left unattended under any circumstances. This should be signed in and out of the office.
- Unwanted paper copies of data, sensitive information or pupil files should be shredded. This also applies to handwritten note that reference any person by name.
- Care to be taken not to leave personal data in printer trays or photocopiers.
- Paper-based records and portable electronic devices, such as laptops and hard drives that contain personal data, are kept in locked cupboard when not in use.
- The school operates a clear desk policy in regard to personal data
- Passwords that are at least 10 characters long containing letters and numbers are used to access school computers, laptops and other electronic devices. Staff and pupils are reminded that they should not reuse passwords from other sites
- Encryption software is used to protect all portable devices and removable media, such as laptops and USB devices
- 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)

These guidelines are clearly communicated and any staff member who intentionally breaches this conduct will be disciplined in line with the policy.

14. 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.

15. 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.

All breaches will be reported to the Data Controller (The Headteacher), who will report to the DPO. The DPO will assess whether the breach needs to be reported to the ICO.

Immediate action will be taken to review how the breach occurred, and make any necessary changes to procedures to ensure that the same problem does not arise again.

16. Training

We are committed to ensuring that staff are aware of data protection policies and legal requirements. All staff and governors are provided with data protection training as part of their induction process. GDPR awareness amongst staff will be refreshed annually, through the sharing of GDPR Fact Sheets. Data protection will also form part of continuing professional development, where changes to legislation, guidance or the school's processes make it necessary.

17. Monitoring arrangements

This policy will be reviewed annually and shared with the full governing board.

- **Appendix 1: Personal data breach procedure**

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

On finding or causing a breach, or potential breach, the staff member, governor or data processor must immediately notify the data protection officer (DPO)

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

- Lost
- Stolen
- Destroyed
- Altered
- Disclosed or made available where it should not have been
- Made available to unauthorised people

Staff and governors will cooperate with the investigation (including allowing access to information and responding to questions). The investigation will not be treated as a disciplinary investigation.

If a breach has occurred or it is likely that is the case, the DPO will alert the headteacher and the chair of governors.

The DPO will make all reasonable efforts to contain and minimise the impact of the breach. Relevant staff members or data processors should help the DPO with this where necessary, and the DPO should take external advice when required (e.g. from IT providers). (See the actions relevant to specific data types at the end of this procedure)

The DPO will assess the potential consequences, based on how serious they are, and how likely they are to happen before and after the implementation of steps to mitigate the consequences

The DPO will work out whether the breach must be reported to the ICO and the individuals affected using the ICO's self-assessment tool

The DPO will document the decisions (either way), in case it is challenged at a later date by the ICO or an individual affected by the breach. Documented decisions are stored on the school's computer system.

Where the ICO must be notified, the DPO will do this via the 'report a breach' page of the ICO website, or through its breach report line (0303 123 1113), within 72 hours of the school's awareness of the breach. As required, the DPO will set out:

- A description of the nature of the personal data breach including, where possible:
    - The categories and approximate number of individuals concerned
    - The categories and approximate number of personal data records concerned
- The name and contact details of the DPO
- A description of the likely consequences of the personal data breach
- A description of the measures that have been, or will be taken, to deal with the breach and mitigate any possible adverse effects on the individual(s) concerned

If all the above details are not yet known, the DPO will report as much as they can within 72 hours of the school's awareness of the breach. The report will explain that there is a delay, the reasons why, and when the DPO expects to have further information. The DPO will submit the remaining information as soon as possible

Where the school is required to communicate with individuals whose personal data has been breached, the DPO will tell them in writing. This notification will set out:

- A description, in clear and plain language, of the nature of the personal data breach
- The name and contact details of the DPO

- A description of the likely consequences of the personal data breach
- A description of the measures that have been, or will be, taken to deal with the data breach and mitigate any possible adverse effects on the individual(s) concerned

The DPO will consider, in light of the investigation and any engagement with affected individuals, whether to notify any relevant third parties who can help mitigate the loss to individuals – for example, the police, insurers, banks or credit card companies

The DPO will document each breach, irrespective of whether it is reported to the ICO. For each breach, this record will include the:

- Facts and cause
- Effects
- Action taken to contain it and ensure it does not happen again (such as establishing more robust processes or providing further training for individuals)

Records of all breaches will be stored on the school's computer system

The DPO and headteacher will meet to review what happened and how it can be stopped from happening again. This meeting will happen as soon as reasonably possible

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

Actions to minimise the impact of data breaches

We set out below the steps we might take to try and mitigate the impact of different types of data breach if they were to occur, focusing especially on breaches involving particularly risky or sensitive information. We will review the effectiveness of these actions and amend them as necessary after any data breach.

Sensitive information being disclosed via email (including safeguarding records)

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

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

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

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