DATA PROTECTION POLICY

2023-2024

Last Update: September 2023

Next Update: September 2024

Contents

1. Aims

First Steps Together aims to ensure that all personal data collected about staff, pupils, parents, proprietors, visitors, and other individuals is collected, stored and processed in accordance with the General Data Protection Regulation (GDPR) and the expected provisions of the Data Protection Act 2018 (DPA 2018) as set out in the Data Protection Bill. This policy applies to all personal data, regardless of whether it is in paper or electronic format.

2. Legislation and guidance

This policy meets the requirements of the GDPR and the expected provisions of the DPA 2018. It is based on guidance published by the Information Commissioner's Office (ICO) on the GDPR and the ICO's code of practice for subject access requests.

It also reflects the ICO's code of practice for the use of surveillance cameras and personal information. In addition, this policy complies with regulation 5 of the Education (Pupil Information) (England) Regulations 2005, which gives parents the right of access to their child's educational record.

3. Definitions

Term	**Definition**
Personal data	Any information relating to an identified, or identifiable, individual. 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

4. The data controller

First Steps Together processes personal data relating to parents, pupils, staff, visitors and others, and therefore is a data controller.

5. Roles and responsibilities

This policy applies to all staff employed by our provision, 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 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 provision data protection issues.
The DPO is also the first point of contact for individuals whose data the provision processes, and for the ICO.

5.2 All staff

Staff are responsible for:

- Collecting, storing and processing any personal data in accordance with this policy
- Informing the provision 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 or 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 provision 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 provision 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 provision can fulfil a contract with the individual, or the individual
  has asked the provision to take specific steps before entering into a contract.
- The data needs to be processed so that the provision can comply with a legal obligation (i.e., DfE census
  information)
- The data needs to be processed to ensure the vital interests of the individual (i.e., to protect someone's life b
  collecting someone's life by collecting data about food allergies or medical conditions)
- The data needs to be processed so that the provision, as a public authority, can perform a task in the public
  interest, or exercise its official authority (i.e., to support pupil learning, to monitor and report on pupil
  attainment progress, to provide appropriate pastoral care and to assess the quality of services)
- The data needs to be processed for the legitimate interests of the provision 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, provision will also meet one of the special category conditions for processing which are set out in the GDPR and Data Protection Act 2018.
First Steps Together (ASE) will always consider the fairness of any data processing. We will ensure it does 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.
- 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.
- ASE will keep data accurate and, where necessary, up to date. Inaccurate data will be rectified or erased when appropriate.
- When staff no longer need the personal data they hold, they must ensure it is deleted or disposed of securely. This will be done in accordance with the provision's record retention schedule.

8. Sharing personal data

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

- There is an issue with a pupil or parent/carer that puts the safety of our staff at risk.
- We need to liaise with other agencies – we will seek consent as necessary before doing this.
- 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:

  1. Only appoint suppliers or contractors which can provide sufficient guarantees that they comply with data protection law
  2. Establish a contract with the supplier or contractor to ensure the fair and lawful processing of any personal data shared
  3. 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.

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.

When 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 provision holds about them. Subject access requests can be submitted in any form, but we may be able to respond to requests more quickly if they are made in writing and 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 DPO.

9.2 Pupil and subject access requests

Personal data about a pupil belongs to that pupil, and not the pupil's parents or carers. For a parent or carer to make a subject access request with respect to their child, the pupil 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 provision 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.

9.3 Responding to subject access requests.

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.
- Will respond without delay and within 1 month of receipt of the request.
- 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 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.
- 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 reasonable 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?
- 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.
  We will also take into account 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.

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 working days of receipt of a written request. All requests must be made in writing to the DPO. The identity of the requestor must be established before the disclosure of any personal information. If the request is for a copy of the educational record, we may charge a fee to cover the costs of supplying it. This right applied 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 actually announced.

11. CCTV

We use CCTV in various locations around the settings to ensure they remain safe. We will adhere to the ICO's code
of practice for the use of CCTV.

We do not need to ask individuals' permission to use CCTV, but we make it clear where individuals are being recorded. Security cameras are clearly visible and accompanied by prominent signs explaining that CCTV is in use.

12. Photographs and videos

As part of our educational activities, we may take photographs and record images of individuals within our provision. We will obtain written consent from parents/carers for photographs and videos to be taken of their child for communication, marketing and promotional materials. We will clearly explain how the photograph and/or video will be used to both the parent/carer and pupil.

Uses may include:

- Within the provision on notice boards and in ASE magazines, brochures, newsletters, etc.
- Outside of the provision by external agencies such as newspapers, campaigns, awards
- Online on the ASE website or social media pages

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.

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:

- 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 staff room 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 site office.
- Passwords that are at least 8 characters long containing letters and numbers are used to access ASE computers, laptops and other electronic devices. Staff and pupils are reminded 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.
- Staff and pupils who store personal information on their personal devices are expected to follow the same security procedures as for ASE-owned equipment (see our staff acceptable use policy).
- 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)

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. We may also use a third party to safely dispose of records on the behalf of ASE. 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

First Steps Together 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 provision context may include, but are not limited to:

- A non-anonymised dataset being published on the ASE website which shows the exam results of pupils
  eligible for the pupil premium.
- Safeguarding information being made available to an unauthorised person.
- The theft of an ASE laptop containing non-encrypted personal data about pupils

16. Training

All staff 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 provision's processes make it necessary.

17. Monitoring arrangements

The DPO is responsible for monitoring and reviewing this policy. This policy will be reviewed and updated, if necessary, when the Data Protection Bill receives royal assent and becomes law (as the Data Protection Act 2018) – if any changes are made to the bill that affect our provision's practice. Otherwise, or from then on, this policy will be reviewed every year and shared with the full governing board.

18. Links with other policies

This data protection policy is linked to our:

- Freedom of information publication scheme
- Safeguarding Policy
- E-Safety & ICT Acceptable Use Policy
- Equality Policy

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 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:
    - o Lost
    - o Stolen
    - o Destroyed
    - o Altered
    - o Disclosed or made available where it should not have been
    - o Made available to unauthorised people.
- The DPO will alert the Senior Leadership Team and 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 DPO will assess the potential consequences, based on how serious they are, and how likely they are to happen.
- The DPO 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 DPO 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:
    - o Loss of control over their data
    - o Discrimination
    - o Identify theft or fraud
    - o Financial loss
    - o Unauthorised reversal of pseudonymisation (for example, key-coding)
    - o Damage to reputation
    - o Loss of confidentiality
    - o Any other significant economic or social disadvantage to the individual(s) concerned

If it's likely that there will be a risk to people's rights and freedoms, the DPO must notify the ICO.

- The DPO 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 within the provision's secure server.
- Where the ICO must be notified, the DPO will do this via the 'report a breach' page of the ICO website within 72 hours. As required, the DPO will set out:
    - o 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*
    - o A description of the likely consequences of the personal data breach 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. 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.
- The DPO 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 DPO will promptly inform, in writing, all individuals whose personal data has been breached. This notification will set out:
    - The name and contact details of the DPO
    - A description of the likely consequences of the personal data breach
    - A description of the measures that have been, or will be, taken to deal with the data breach and mitigate any possible adverse effects on the individual(s) concerned.
- The DPO 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 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 within the provision's secure server.

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

Actions to minimise the impact of data breaches.

We will take the actions set out below to mitigate the impact of different types of data breach, 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 to recall it.
- In any cases where the recall is unsuccessful, the DPO will 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 ensure we receive 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.

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

- Details of pupil premium interventions for named pupils being published on the ASE website.
- Non-anonymised pupil exam results or staff pay information being shared.