



General Data Protection Regulation (GDPR) Policy

Contents

1. Aims	2
2. Legislation and guidance	2
3. Definitions.....	2
4. The Data Controller.....	2
5. Roles and responsibilities	3
6. Data protection principles	3
7. Collecting personal data	4
8. Sharing personal data.....	5
9. Subject access requests and other rights of individuals	5
10 Photographs and videos	7
11. Data protection by design and default.....	7
12. Data security and storage of records.....	8
13. Disposal of records	8
14. Personal data breaches	8
15. Training.....	8
16. Monitoring arrangements	8
17. Links with other policies	9
18. Policy status and review.....	9
Appendix 1: Personal data breach procedure.....	10

1. Aims

1.1 Aspire Farm School aims to ensure that all personal data collected about staff, students, parents/carers, volunteers, visitors, and other individuals is collected, stored, and processed in accordance with the UK data protection law.

1.2 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 UK General Data Protection Regulation (UK GDPR) – the EU GDPR was incorporated into UK legislation, with some amendments, by The Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2020.

3. Definitions

3.1 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.

3.2 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.

3.3 Data subject

The identified or identifiable individual whose personal data is held or processed.

3.4 Data controller

A person or organisation that determines the purposes and the means of processing of personal data.

3.5 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.

3.6 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

4.1 Aspire Farm School determines the purpose of processing personal data relating to parents/carers, students, staff, volunteers, visitors, and others, and therefore is a data controller.

4.2 Aspire Farm School is registered as a Data Controller with the Information Commissioner's Office (ICO) and will pay the data protection fee for registration annually to the ICO or as otherwise legally required.

5. Roles and Responsibilities

5.1 This policy applies to all staff employed by Aspire Farm School. Staff who do not comply with this policy may face disciplinary action.

5.2 Aspire Farm School has overall responsibility for ensuring compliance with all relevant data protection obligations.

5.3 Data Protection Officer (DPO)

The Data Protection Officer is responsible for advising on the implementation of this policy, monitoring compliance with data protection law, and developing related policies and guidelines where applicable.

The DPO for Aspire Farm School is Katie Jackson, Board of Directors, Aspire Farm School. She is contactable via email at k.jackson@aspirefarmschool.co.uk

5.4 The DPO's responsibilities are:-

- To inform and advise Aspire Farm School and its employees about their obligations to comply with the GDPR and other data protection laws.
- To monitor compliance with the GDPR and other data protection laws, including managing internal data protection activities, advising on data protection impact assessments, training staff, and conducting internal audits.
- To be the first point of contact for the ICO and for individuals whose data is processed by Aspire Farm School.

5.5 All staff are responsible for:-

- Collecting, storing, and processing any personal data in accordance with this policy
- Informing the relevant professional service of any changes to their personal data, such as a change of address
- Contacting the DPO (via k.jackson@aspirefarmschool.co.uk) 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 UK
 - If there has been a data breach
 - 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 must be complied with. This policy sets out how Aspire Farm School aims to comply with these principles. 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

7. Collecting Personal Data

7.1 Lawfulness, fairness, and transparency.

Personal data will only be processed when there is one of five 'lawful bases' (legal reasons) to do so under data protection law:-

- The data needs to be processed so that Aspire Farm School can fulfil a contract with the individual, or the individual has asked Aspire Farm School to take specific steps before entering into a contract
- The data needs to be processed to comply with a legal obligation
- The data needs to be processed to ensure the vital interests of the individual or another person (e.g. to protect someone's life)
- The data needs to be processed so that Aspire Farm School, as a provider of alternative provision, can perform a task in the public interest or exercise its authority.
- The individual (or their parent/carer when appropriate in the case of a student) has freely given clear consent

7.2 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 student) 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 protections 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 the 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 the law
- The data needs to be processed for archiving purposes, scientific or historical research purposes, or statistical purposes, and the processing in the public interest

7.3 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 student) 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

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

7.5 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.

7.6 Limitation, minimization, and accuracy

7.6.1 Only personal data for specified, explicit, and legitimate reasons will be collected. The reasons for collecting the data will be explained to the individuals when the data is first collected. If personal data is to be used for reasons other than those given when it was first obtained, the individuals concerned will be informed before it is used and consent sought.

7.6.2 Staff must only process personal data where it is necessary in order to do their jobs. When staff no longer need the personal data they hold, they must ensure it is deleted or anonymized. This will be done in accordance with Aspire Farm School's Record Management Policy.

8. Sharing Personal Data

8.1 Aspire Farm School will not normally share personal data with anyone else, but may do so where:-

- There is an issue with a student or parent/carer that puts the safety of our staff at risk
- We need to liaise with other agencies, including safeguarding, welfare, and health services, to carry out tasks in the public interest or for official functions
- Our suppliers or contractors need data to enable us to provide services to our staff and students – for example, IT companies. When doing this, we will:-
 - Only appoint suppliers or contractors who can provide sufficient guarantees that they comply with UK data protection law
 - Establish a data processing agreement 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, and ensure that they keep the data secure and not use it for their own purposes

8.2 We will also share personal data with law enforcement and government bodies where we are legally required to do so, including for:-

- The prevention or detection of crime and/or fraud
- The apprehension or prosecution of offenders
- The assessment or collection of tax owed to HMRC
- In connection with legal proceedings
- Where the disclosure is required to satisfy our safeguarding obligations
- Research and statistical purposes, as long as personal data is sufficiently anonymized or pseudonymized
- In an emergency, to protect the vital interests of the individual concerned

9. Subject Access Requests and Other Rights of Individuals

9.1 Individuals have a right to make a subject access request to gain access to personal information that the school holds about them.

9.2 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 is not possible, the criteria used to determine this period
- The source of the data, if not the individual
- Whether any automated decision-making is being applied to their data, and what the significance and consequences of this might be for the individual

9.3 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

9.4 If staff receive a subject access request, they must immediately forward it to the DPO.

9.5 Children and subject access requests

9.5.1 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.

9.5.2 Children aged 13 and above can generally understand their rights and the implications of a subject access request. Therefore, most subject access requests from parents or carers of students at our school may not be granted without the express permission of the pupil.

9.5.3 Children aged below 13 are not generally considered mature enough to understand their rights and the implications of a subject access request. Therefore, parents or carers can make subject access requests on behalf of students of this age.

9.6 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 (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.

9.7 If the request is unfounded or excessive, we may refuse to act on it, or charge a reasonable fee which takes into account administrative costs. A request will be deemed to be unfounded or excessive if it is repetitive or asks for further copies of the same information.

9.8 Other data protection rights of the individual

9.8.1 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 (where the lawful basis for processing is consent)
- Ask us to rectify, erase or restrict processing of their personal data (in certain circumstances)
- 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
- Request a copy of agreements under which their personal data is transferred outside of the UK
- Challenge processing which has been justified on the basis of public interest
- Request a copy of personal data about them that is held by us
- Be informed of the existence of automated decision-making, including profiling, and the significance and consequences of such processing for them.

- Lodge a complaint with the ICO if they think that we have failed to comply with their data protection rights

9.8.2 Individuals should submit any request to exercise these rights to the DPO (k.jackson@aspirefarm.com). If staff receive such a request, they must immediately forward it to the DPO.

10. Photographs and Videos

10.1 Aspire Farm School will obtain written consent from parents/carers or students aged 13 and above, for photographs and videos to be taken of students 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 student. Written consent will be kept on record and regularly reviewed. If we do not receive explicit consent, we will not use the photographs or videos for these purposes.

10.2 Uses may include:-

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

10.3 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.

10.4 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.

10.5 See our child protection and safeguarding policy for more information on our use of photographs and videos.

11. Data Protection by Design and Default

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 doing so in the least intrusive way possible
- Conducting Data Protection Impact Assessments (DPIAs) where the processing is likely to result in a high risk to individuals' rights and freedoms. DPIAs will be conducted with the advice of the DPO and involve relevant stakeholders
- 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. Records of attendance will be kept to demonstrate compliance
- Regularly conducting reviews and audits to test our privacy measures and make sure we are compliant
- Maintaining records of our processing activities, including:-
 - For the benefit of data subjects, making available the name and contact details of our school and 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, data subject, and processing activities, with appropriate justifications and details.

12. Data Security and Storage of Records

Aspire Farm School 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. Measures to protect personal data include:-

- Ensuring the physical security of our premises
- Using secure access controls to systems where personal data is stored
- Ensuring our IT systems are protected against malware and data breaches, including regular software updates, anti-virus protection, and secure networks
- Encrypting and pseudonymised data where appropriate, ensuring it is unintelligible in the event of unauthorised access
- Limiting access to personal data to those staff members who need to use it in their work
- Storing paper-based records in secure cabinets
- Password-protecting laptops and other mobile devices that store personal data
- Training staff on how to handle personal data securely and on the importance of confidentiality

13. Disposal of Records

Personal data that is no longer needed will be disposed of securely. Hard copy personal data will be shredded, and electronic copies will be permanently deleted from our systems.

14. Personal Data Breaches

14.1 Aspire Farm School will make all reasonable endeavours to ensure that there are no personal data breaches.

14.2 In the event of a suspected data breach, we will follow the procedure set out in **Appendix 1**.

14.3 When appropriate, we will report the data breach to the ICO within 72 hours. Such breaches in a school context may include, but are not limited to:-

- Safeguarding information being made available to an unauthorised person
- The theft of a school laptop containing non-encrypted personal data about students.

15. Training

15.1 All staff and directors are provided with data protection training as part of their induction process.

15.2 Data protection training will also be included as part of the school's continuing professional development (CPD) programme.

15.3 Regular data protection training will be provided to all staff, and records of attendance will be kept to demonstrate compliance.

16. Monitoring Arrangements

16.1 The DPO is responsible for monitoring and reviewing this policy.

16.2 This policy will also be updated as necessary to reflect changes in legislation, guidance, or the data protection practices of the school.

17. Links with Other Policies

This data protection policy is linked to the following policies:-

- Confidentiality & Privacy Policy

- Child Protection and Safeguarding Policy

18. Policy Status and Review

Written by:	Caroline Tasker, Director
Owner:	Caroline Tasker, Director
Status:	V1= 18/06/2024 Submitted to the Board of Directors, Aspire Farm School
Date approved:	V1= 20/06/2024
Date reviewed:	
Next review date:	June 2026

Appendix 1: Personal Data Breach Procedure

Step 1: Containment and Recovery

- The person who discovers/receives a report of a breach must inform the DPO immediately.
- The DPO will investigate the breach, identify the root cause, and take steps to contain the breach and recover any lost or compromised data.
- The DPO will assess whether further steps are required to mitigate the effects of the breach and prevent a recurrence.

Step 2: Risk Assessment

- The DPO will assess the potential adverse consequences for individuals, based on how serious or substantial these are and how likely they are to happen.
- The DPO will decide whether the breach must be reported to the ICO.

Step 3: Notification of the Breach

- If the breach is likely to result in a risk to the rights and freedoms of individuals, the DPO will notify the ICO within 72 hours of becoming aware of the breach.
- The DPO will ensure that appropriate records are maintained of the breach and any actions taken to mitigate its effects.

Step 4: Evaluation and Response

- The DPO will assess the effectiveness of Aspire Farm School's response to the breach, identify any weaknesses, and take steps to prevent recurrence.
- The DPO will report findings and recommendations to the governing body for further action, if necessary
