Apple Tree Farm Services CIC, High Bickington, Umberleigh, Devon, EX37 9BJ
Tel: 01769 560095/07908783759
Email: contact@appletreefarmservices.co.uk www.appletreefarmservices.co.uk

Apple Tree Farm Services CIC

Data Protection Policy

Scope

For purposes of the applicable data protection laws *Apple Tree Farm Services CIC* is the "data controller". This means that *Apple Tree Farm Services CIC* determines the purposes for which, and the way, your data is processed.

Introduction

Apple Tree Farm Services CIC aims to ensure that all personal data collected about staff, children, parents, trustees, visitors and other individuals is collected, stored and processed in accordance with UK data protection law.

This policy applies to all personal data, regardless of whether it is in paper or electronic format.

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

• Data Protection Act 2018 (DPA 2018)
It is based on guidance published by the Information Commissioner's Office (ICO) on the GDPR and guidance from the Department of Education (DfE) on Generative artificial intelligence (AI) in education - GOV.UK

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. This policy complies with our Articles of Association and Governance Documents.

The Data Controller

The farm processes personal data relating to parents, children, staff, trustees, members, visitors and others, and therefore is a data controller. The farm is registered with the ICO and will renew this registration annually or as otherwise legally required.

Roles and responsibilities

This policy applies to all staff employed by the farm, and to external organisations or individuals working on our behalf. Staff who do not comply with this policy may face disciplinary action.

The Board

The board of directors has overall responsibility for ensuring that our farm complies with all relevant data protection obligations.

Data Protection Officer

The nominated data protection officer (DPO) is responsible for overseeing the implementation of this policy, monitoring our compliance with data protection law, and guidelines where applicable.

They will offer advice, audit reports and recommendations on Farm data protection.
The DPO is also the first point of contact for individuals whose data the Farm processes, and for the ICO.

Our nominated DPO is Brenda Pedroni and contactable via email on brenda@appletreefarmservices.co.uk

All staff

Staff are responsible for:

• Collecting, storing and processing any personal data in accordance with this policy

• Informing the farm 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 UK
- 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

The UK GDPR is based on data protection principles that our farm 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 farm 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 farm can fulfil a contract with the individual, or the individual has asked the farm to take specific steps before entering into a contract
• The data needs to be processed so that the farm can comply with a legal obligation
• The data needs to be processed to ensure the vital interests of the individual e.g. to protect someone's life
• The data needs to be processed so that the farm, as a public authority, can perform a task in the public interest, and carry out its official functions
• The data needs to be processed for the legitimate interests of the farm 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.

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.

When staff no longer need the personal data they hold, they must ensure it is deleted or anonymised.

We will keep data accurate and, where necessary, up to date. Inaccurate data will be rectified or erased when appropriate.

This will be done in accordance with the farm's record retention schedule.

Our processing of special categories of personal data and criminal offence data

As part of our statutory functions, we process special category data and criminal offence data in accordance with the requirements of Articles 9 and 10 of the UK General Data Protection Regulation (UK GDPR) and Schedule 1 of the Data Protection Act 2018 (DPA 2018).

Special Category Data

Special category data is defined at Article 9 of the UK GDPR as personal data revealing:

- Racial or ethnic origin
- Political opinions
- Religious or philosophical beliefs
- Trade union membership
- Genetic data
- Biometric data for the purpose of uniquely identifying a natural person
- Data concerning health
- Data concerning a natural person's sex life or sexual orientation

Criminal Conviction Data

Article 10 of the UK GDPR covers processing in relation to criminal convictions and offences or related security measures. In addition, section 11(2) of the DPA 2018 specifically confirms that this includes personal data relating to the alleged commission of offences or proceedings for an offence committed or alleged to have been committed, including sentencing. This is collectively referred to as 'criminal offence data'.

Appropriate Policy Document (APD)

Some of the Schedule 1 conditions for processing special category and criminal offence data require us to have an Appropriate Policy Document (APD) in place, setting out and explaining our procedures for securing compliance with the principles in Article 5 and policies regarding the retention and erasure of such personal data.

This section of our Data Protection Policy document explains our processing and satisfies the requirements of Schedule 1, Part 4 of the DPA 2018.

In addition, it provides some further information about our processing of special category and criminal offence data where a policy document isn't a specific requirement. The information supplements our privacy notices.

Conditions for processing special category and criminal offence data

We process special categories of personal data under the following UK GDPR

Articles:

1. Article 9(2)(a) – explicit consent
In circumstances where we seek consent, we make sure that the consent is unambiguous and for one or more specified purposes, is given by an affirmative action and is recorded as the condition for processing.

Examples of our processing include staff dietary requirements and health information we receive from our children who require a reasonable adjustment to access our services.

2. Article 9(2)(b) – where processing is necessary for the purposes of performing or exercising obligations or rights which are imposed or conferred by law on the Farm or the data subject in connection with employment, social security or social protection.
Examples of our processing include staff sickness absences.

3. Article 9(2)(c) – where processing is necessary to protect the vital interests of the data subject or of another natural person.
An example of our processing would be using health information about a pupil or member of staff in a medical emergency.

4. Article 9(2)(f) – for the establishment, exercise or defence of legal claims.
Examples of our processing include processing relating to any employment tribunal or other litigation.

5. Article 9(2)(g) - reasons of substantial public interest.
As a farm we are a publicly funded body and provide a safeguarding role to young and vulnerable people. Our processing of personal data in this context is for the purposes of substantial public interest and is necessary for the carrying out of our role.
Examples of our processing include the information we seek or receive as part of investigating an allegation.

6. Article 9(2)(j) – for archiving purposes in the public interest.

The relevant purpose we rely on is Schedule 1 Part 1 paragraph 4 – archiving.
An example of our processing is the transfers we make to our archives as set out in our Records Management Policy.

We process criminal offence data under Article 10 of the UK GDPR

Examples of our processing of criminal offence data include pre-employment checks and declarations by an employee in line with contractual obligations.

Processing which requires an Appropriate Policy Document

Almost all the substantial public interest conditions in Schedule 1 Part 2 of the DPA 2018, plus the condition for processing employment, social security and social protection data, require an APD (see Schedule 1 paragraphs 1 and 5).

This section of the policy is the APD for the farm. It demonstrates that the processing of special category (SC) and criminal offence (CO) data based on these specific Schedule 1 conditions is compliant with the requirements of the UK GDPR Article 5 principles. Our retention with respect to this data is documented in our retention schedules.

Description of data processed

We process the special category data about our employees that is necessary to fulfil our obligations as an employer. This includes information about their health and wellbeing, ethnicity, photographs and their membership of any union. Further information about this processing can be found in our staff privacy notice.

We process the special category data about the children in our care and other members of our community that is necessary to fulfil our obligations as a farm and for safeguarding and care. This includes information about their health and wellbeing, ethnicity, photographs and other categories of data relevant to the provision of care. Further information about this processing can be found in our pupil privacy notice.

We also maintain a record of our processing activities in accordance with Article 30 of the UK GDPR.

Schedule 1 conditions for processing

Special category (SC) data

We process SC data for the following purposes in Part 1 of Schedule 1:

• Paragraph 1(1) employment, social security and social protection.
We process SC data for the following purposes in Part 2 of Schedule 1. All processing is for the first listed purpose and might also be for others dependent on the context:
• Paragraph 6(1) and (2)(a) statutory, etc. purposes
• Paragraph 18(1) – safeguarding of children and of individuals at risk

Criminal offence data

We process criminal offence data for the following purposes in parts 1, 2 and 3 of Schedule 1:
• Paragraph 1 – employment, social security and social protection
• Paragraph 6(2)(a) – statutory, etc. purposes
• Paragraph 12(1) – regulatory requirements relating to unlawful acts and dishonesty etc
• Paragraph 18(1) – safeguarding of children and of individuals at risk
Paragraph 36 – Extension of conditions in part 2 of this Schedule referring to substantial public interest

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 including, but not limited to, Health Care Professionals – we will seek consent as necessary before doing this if appropriate
- Our suppliers or contractors need data to enable us to provide services to our staff and children – for example, IT companies. When doing this, we will:
- Only appoint suppliers or contractors which can provide sufficient guarantees that they comply with UK data protection law
- Establish a data sharing agreement with the supplier or contractor, either in the contract or as a standalone agreement, 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

Where there are recognised legitimate interests for processing personal data for crime prevention, safeguarding, responding to emergencies, and other specified legitimate interests. We will 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 children or staff. Where we transfer personal data internationally, we will do so in accordance with UK data protection law.

Subject access requests and other rights of individuals

Subject access requests

Individuals have a right to make a 'subject access request' to gain access to personal information that the farm holds about them. When an individual asks for their personal data, they do not have to call it a SAR. It could be in the form of a complaint, or could quote other legislation, such as Freedom of information request. To submit an SAR please contact the nominated Data Protection Officer via brenda@appletreefarmservices.co.uk or visit ICO Website Make A subject access request

Information held 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

A requester can ask for any personal data that relates to:

• themselves
• someone they have parental responsibility for
• someone they have permission to act on behalf of

Subject access requests can be submitted verbally over the telephone or face-to-face or in writing, either by letter, text, or email.

They should 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 nominated DPO. If a request is non-specific, i.e. 'all the information you hold', we may ask for clarification of what specific information the requester is looking for.

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 13 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 children at our farm 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.

Children aged 13 and above are generally 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 children at our farm may not 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.

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 acknowledge receipt of the request as soon as possible and will respond to the SAR within 1 month of receipt of the request. However please note we will 'stop the clock' to pause the response time if we need more information from you regarding your request. Once the information is received the response time will continue.
• Will provide the information free of charge. However, if the request is excessive, we may charge a reasonable fee to cover administration costs.
• 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, safeguarding records, 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

When we refuse a request, we will tell the individual why and tell them they have the right to raise concerns with our nominated Data Protection Officer or complain to the ICO.

The UK GDPR does not prevent a data subject making a subject access request via a third party. Requests from third parties are dealt with as follows:

• In these cases, we need to be satisfied that the third party making the request is entitled to act on behalf of the data subject
• It is the third party's responsibility to provide evidence of this entitlement
• This might be a written authority to make the request, or it might be a more general power of attorney
• If there is no evidence that the third party is authorised to act on behalf of the data subject, we are not required to respond to the SAR
• However, if we are able to contact the data subject, we will respond to them directly to confirm whether they wish to make a SAR

Subject Access Request Data Searches

When responding to a Subject Access Request, we will carry out reasonable and proportionate searches to locate personal data. (Article 15 (1A) UK GDPR) This means we will:

• Identify systems and records where relevant personal data is likely to be held.
• Avoid excessive or irrelevant searches that would place an undue burden on the farm.
• Consider the nature of the request, the context of the data, and the effort required to retrieve it.

This approach ensures we meet our obligations while balancing practicality and fairness.

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. A request will be deemed to be unfounded or excessive if it is repetitive or asks for further copies of the same information.

Requests will be processed in accordance with the Department for Education guidance Dealing with subject access requests (SARS). This guidance also refers to “Dealing with information already held by the requestor”: Data protection in schools - Dealing with subject access requests (SARs)

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 (see section 7), 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 (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
• 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)
• Request a copy of agreements under which their personal data is transferred outside of the UK
• 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)
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.

Under Section 164A of the Data Protection Act 2018, you have a statutory right to complain if you believe your personal data has been handled inappropriately.

If you wish to raise a concern or complaint about how we process your personal data, please contact us directly. We will acknowledge your complaint within 30 days of receipt and take appropriate steps to investigate and respond without undue delay.

If you are not satisfied with our response, you may escalate your complaint to the Information Commission at: Information Commissioner's Office

Handling of other information rights requests

Other information rights requests, including changing, deleting or restricting the processing of personal information. The individual has a right to access or amend the personal data any organisation holds about them. Individuals, including children, have several information rights relating to personal data an organisation may hold about them.
A guide to individual rights

Information rights request that someone might make include asking to:

• change inaccurate personal information the farm holds
• remove their personal information or record
• restrict the processing of their personal information
• stop processing their personal information (right to object)

Information rights requests relating to personal data can be submitted verbally over the telephone or face-to-face or in writing, either by letter, text, or email.
We will respond to any information rights request within one calendar month. If the case is complex we can extend the response deadline by an extra 2 calendar months.
Information rights requests only apply to the personal data we hold when we get the request. Individuals have the right to request changes or restrictions to personal information, but the farm is not obliged to make changes to data in certain circumstances.

Individuals should submit any request to exercise these rights to the nominated DPO. If staff receive such a request, they must immediately forward it to the nominated DPO.

Parental requests to see the educational record

An education record includes:

• Records of the pupil's academic achievements
• Correspondence about the pupil from teachers, local authority (LA) employees and educational psychologists engaged by the governing board
• Information from the pupil and their parent(s)

It doesn't include any information about the pupil that a teacher keeps solely for their own use. Access to education records is a separate right and is not covered by Data Protection legislation. Unlike the right to access under Data Protection legislation, this right does not extend to children. In England, schools are regulated by The Education (Pupil Information) (England) Regulations 2005. Those with parental authority can apply to the school to view an education record or receive a copy. In England, this right only

applies to all local authority schools, and all special schools, including those which are not maintained by a local authority. Independent schools, academies, alternative provision settings and free schools are not obliged to respond to a request for access to a pupil's education record under this legislation.
The farm will supply the educational records within one month of receipt of the request to parents, or those with parental responsibility.
If the request is for a copy of the educational record, the farm may charge a fee to cover the cost of supplying it. This right applies if 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.

Biometric Recognition Systems

The Farm does not collect or otherwise process biometric data.

CCTV

We use CCTV in various locations around the farm to ensure it remains 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.

Any enquiries about the CCTV system should be directed to the administration team via admin@appletreefarmservices.co.uk

Photographs and videos

As part of our farm activities, we may take photographs and record images of individuals within our farm recording systems, in line with the term stated in the farm's Photography and Filming Policy.

We will obtain written consent from parents/carers for photographs and videos to be taken of their child for communication, marketing and promotional materials. 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.

Uses may include:
• Within the farm on notice boards and in farm magazines, brochures, newsletters, etc
• Outside of the farm by external agencies such as the newspapers, campaigns
• Online on our farm 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.

Any photographs and videos taken by parents/carers at farm events for their own personal use are not covered by data protection legislation. However, we will ask that photos or videos with other children are not shared publicly on social media for safeguarding reasons, unless all the relevant parents/carers (or children where appropriate) have agreed to this.

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

Artificial intelligence (AI)

Artificial intelligence (AI) tools are now widespread and easy to access. The farm recognises that AI has many uses to help children learn but also poses risks to sensitive and personal data.

The farm will only use AI tools that have been risk assessed, evaluated and are farm approved. Personal and/or sensitive data will not be entered into a generative AI tool. The farm will treat this as a data breach. Please see Appendix 1 for procedure.

Data protection by design and default

We will put measures in place to show that we have integrated data protection into all our data processing activities, including:

• Appointing a 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 (see section 5)
• Completing data protection impact assessments (DPIAs) where the farm's processing of personal data presents a high risk to rights and freedoms of individuals, and when introducing new technologies (the DPO will advise on this process – see section 13.1) (The DPO will advise on this process)
• 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
• Maintaining records of our processing activities, including:

o For the benefit of data subjects, making available the name and contact details of our nominated DPO and all information we are required to share about how we use and process their personal data (via our privacy notices)

o For all personal data that we hold, maintaining an internal record of the type of data, data subject, how and why we are using the data, any third-party recipients, how and why we are storing the data, retention periods and how we are keeping the data secure

Data Protection Impact Assessments (DPIAs)

A Data Protection Impact Assessment (DPIA) is a process to help us identify and minimise the data protection risks of a project.

We will do a DPIA for processing that is likely to result in a high risk to individuals as well as any other major project which requires the processing of personal data.
It is vital that the DPIA is completed before processing is commenced to ensure that all risks are identified and mitigated as much as possible.

Our DPIA will:

• describe the nature, scope, context, and purposes of the processing
• assess necessity, proportionality, and compliance measures
• identify and assess risks to individuals
• identify any additional measures to mitigate those risks

To assess the level of risk, we will consider both the likelihood and the severity of any impact on individuals. High risk could result from either a high probability of some harm, or a lower possibility of serious harm.

We will consult our data protection officer and, where appropriate, individuals and relevant experts. We may also need to consult with relevant processors.

If we identify a high risk that we cannot mitigate, we will consult the ICO before starting the processing.

We will implement the measures we identified from the DPIA, and integrate them into our policies, procedures, and practice.
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:

• Access to all our files and folders on SharePoint are set out in a way to limit access to sensitive or personal data through the use of tiered security access. Green libraries are accessible by all staff, and contain non-personal, non-sensitive information. Red libraries are access controlled to protect personal and sensitive data in compliance with GDPR. Access is granted based on role and necessity
• There should be NO paper files

• There should be NO paper files of personal data regarding children other than current information which should be shredded or passed securely to their new school as soon as the pupil leaves. Old archives, pre-farm should be stored securely
• 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, 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 farm office
• Passwords that are at least 8 characters long containing letters and numbers are used to access farm computers, laptops and other electronic devices. Staff and children are reminded to change their passwords at regular intervals

Removable Media

Removable media such as memory sticks and cards, CDs, DVDs, diskettes and other portable memory devices allow us to share and move information both inside and outside Wave but they can easily be lost, stolen or damaged. We need safeguards in place to ensure sensitive and personal data is stored securely and that the farm's network is protected from viruses and malware. Any removable media must be encrypted.

Users should only use removable media to store sensitive or personal data on an exceptional and short-term basis and it should be deleted as soon as possible. Users should make sure the anti-virus and malware checking software is working and up to date on any computers they plan to connect removable media to. If users are transferring data from one computer to another, they must check the anti-virus and malware checking software on both machines first.

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 farm's behalf. If we do so, we will require the third party to provide sufficient guarantees that it complies with data protection law.

Personal data breaches

The farm 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 our context may include, but are not limited to:

• A non-anonymised dataset being published on the farm website which shows the exam results of children eligible for the pupil premium
• Safeguarding information being made available to an unauthorised person
• The theft of a farm laptop containing non-encrypted personal data about children
• The transfer of data or information to those who are not entitled to receive it, e.g. sending information to the wrong recipient or discussing sensitive information in earshot of other people
• Attempts (either failed or successful) to gain unauthorised access to data or information, e.g. 'phishing' whereby users are sent an email requesting their username or password
• Unauthorised access to a system, e.g. allowing a third party to access information
• Not protecting physical access to information, e.g. leaving confidential papers in full view on your desk while you are in a meeting

Training

All staff and trustees are provided with inhouse 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 farm's processes make it necessary.

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, data processor, trustees, members and/or representatives must immediately notify the DPO giving as many details as possible.

The DPO will investigate the report, and determine whether a breach has occurred. Staff, trustees, members and representatives will be expected to cooperate with an investigation, this will not be treated as a disciplinary investigation. 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

The DPO will alert the board of directors and will then 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 seek external advice (e.g. from Equinoxx) if necessary when trying to contain and minimise the impact of the breach. The DPO will assess the potential consequences of the breach, both before and after the

implementation of mitigating steps, based on how serious they are, and how likely they are to happen and will work out whether the breach must be reported to the ICO. This must be judged on a case-by-case basis. The DPO will use the ICO's self-assessment tool to work out whether a breach must be reported to the ICO.

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 (eg. emotional distress), including through:
• Loss of control over their data
• Discrimination
• Identify theft or fraud
• Financial loss
• Unauthorised reversal of pseudonymisation (for example, key-coding)
• Damage to reputation
• Loss of confidentiality
• 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.

If the farm is required, under Data Protection Legislation, to notify the Information Commissioner or a Data Subject of a Personal Data Breach in relation to the farm, then within 48 hours of the breach occurring the DPO will inform the relevant parties.

Where the ICO must be notified, DPO will do this via the 'report a breach' page of the ICO website within 72 hours. As required, DPO will set out:

• A description of the nature of the personal data breach including, where possible:
o The categories and approximate number of individuals concerned
o 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. 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. They 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, documenting 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 with the Data Breach Register within the farm's shared drive.

The DPO and relevant parties will meet to review what happened and how it can be stopped from happening again. This meeting will happen as soon as reasonably possible. 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, trustees, members and representatives who receive personal data sent in error must alert the sender and the DPO as soon as they become aware of the error
• 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 endeavour to obtain a written response from all the individuals who received the data, confirming that they have complied with this request and 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.

You may contact: Brenda Pedroni, Director at Apple Tree Farm Services CIC on Brenda@appletreefarmservices.co.uk

Bleonard

Farm Manager

This policy was last reviewed on: 06/02/2026