



GDPR Policy

Introductions

Corn Close Care Farm takes the security and privacy of your data seriously. We need to gather and use information or 'data' about you as part of our business and to manage our relationship with you. We intend to comply with our legal obligations under the **Data Protection Act 2018** (the '2018 Act') and the **EU General Data Protection Regulation** ('GDPR') in respect of data privacy and security. We have a duty to notify you of the information contained in this policy.

The General Data Protection Regulation (GDPR) ensures a balance between an individual's rights to privacy and the lawful processing of personal data undertaken by organisations in the course of their business. It aims to protect the rights of individuals about whom data is obtained, stored, processed or supplied and requires that organisations take appropriate security measures against unauthorised access, alteration, disclosure or destruction of personal data.

Corn Close Care Farm will protect and maintain a balance between data protection rights in accordance with the GDPR. This policy sets out how we handle the personal data of our pupils, parents, suppliers, employees, workers and other third parties.

This policy does not form part of any individual's terms and conditions of employment with Corn Close Care Farm and is not intended to have contractual effect. Changes to data protection legislation will be monitored and further amendments may be required to this policy in order to remain compliant with legal obligations.

This policy applies to current and former employees, workers, volunteers, service users and their parents/carers, apprentices and consultants. If you fall into one of these categories then you are a 'data subject' for the purposes of this policy.

Corn Close Care Farm is a '**data controller**' for the purposes of your personal data. This means that we determine the purpose and means of the processing of your personal data. We will only hold data for as long as necessary for the purposes for which we collected it.

This policy explains how Corn Close Care Farm will hold and process your information. It explains your rights as a data subject. It also explains your obligations when obtaining, handling, processing or storing personal data in the course of volunteering for, working for, or on behalf of, Corn Close Care Farm.

DEFINITIONS

Personal data - personal data is any information relating to an individual where the individual can be identified (directly or indirectly) from that data alone or in combination with other identifiers we possess or can reasonably access. This includes special category

data and pseudonymised personal data but excludes anonymous data or data that has had the identity of an individual permanently removed.

Personal data can be factual (for examples a name, email address, location or date of birth) or an opinion about that person's actions or behaviour.

Personal data will be stored either electronically or as part of a structured manual filing system in such a way that it can be retrieved automatically by reference to the individual or criteria relating to that individual.

Special Category Data - previously termed "Sensitive Personal Data", Special Category Data is similar by definition and refers to data concerning an individual Data Subject's racial or ethnic origin, political or religious beliefs, trade union membership, physical and mental health, sexuality, biometric or genetic data and personal data relating to criminal offences and convictions.

Data Subject - an individual about whom such information is stored is known as the Data Subject. It includes but is not limited to employees, volunteers and visitors.

Data Controller - the organisation storing and controlling such information (i.e. Corn Close Care Farm) is referred to as the Data Controller.

Processing - processing data involves any activity that involves the use of personal data. This includes but is not limited to: obtaining, recording or holding data or carrying out any operation or set of operations on that data such as organisation, amending, retrieving using, disclosing, erasing or destroying it. Processing also includes transmitting or transferring personal data to third parties.

Automated Processing - any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to an individual, in particular to analyse or predict aspects concerning that individual's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.

An example of automated processing includes profiling and automated decision making. Automatic decision making is when a decision is made which is based solely on automated processing which produces legal effects or significantly affects an individual. Automated decision making is prohibited except in exceptional circumstances.

Data Protection Impact Assessment (DPIA) - DPIAs are a tool used to identify risks in data processing activities with a view to reducing them.

Criminal Records Information - this refers to personal information relating to criminal convictions and offences, allegations, proceedings, and related security measures.

Corn Close Care Farm will process data as follows:

Data Protection Principles - Corn Close Care Farm are responsible for and adhere to the principles relating to the processing of personal data as set out in the GDPR.

The principles Corn Close Care Farm must adhere to are: -

- Personal data must be processed lawfully, fairly and in a transparent manner;
- Personal data must be collected only for specified, explicit and legitimate purposes;

- Personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed;
- Personal data must be accurate and, where necessary, kept up to date;
- Personal data must not be kept in a form which permits identification of data subjects for longer than is necessary for the purposes for which the data is processed;
- Personal data must be processed in a manner that ensures its security using appropriate technical and organisational measures to protect against unauthorised or unlawful processing and against accidental loss, destruction or damage.

Sharing Personal Data

Corn Close Care Farm will generally not share personal data with third parties unless certain safeguards and contractual arrangements have been put in place. These include if the third party: -

- Sharing the personal data complies with the privacy notice that has been provided to the data subject and, if required, the data subject's consent has been obtained;
- the third party has agreed to comply with the required data security standards, policies and procedures and put adequate security measures in place;

There may be circumstances where Corn Close Care Farm is required either by law or in the best interests of a visitor, parent/carer or staff to pass information onto external authorities, for example, the local authority, Ofsted or the department of health. These authorities are up to date with data protection law and have their own policies relating to the protection of any data that they receive or collect.

Transfer of Data Outside the European Economic Area (EEA)

The GDPR restricts data transfers to countries outside the EEA in order to ensure that the level of data protection afforded to individuals by the GDPR is not undermined.

Corn Close Care Farm will not transfer data to another country outside of the EEA without appropriate safeguards being in place and in compliance with the GDPR. All staff must comply with the guidelines on transferring data outside of the EEA.

DATA SUBJECT'S RIGHTS AND REQUESTS

Personal data must be made available to data subjects and data subjects must be allowed to exercise certain rights in relation to their personal data.

The rights data subjects have in relation to how Corn Close Care Farm handle their personal data are set out below: -

1. (Where consent is relied upon as a condition of processing) To withdraw consent to processing at any time;
2. Receive certain information about the provision's processing activities;
3. Request access to their personal data that we hold;
4. Prevent our use of their personal data for marketing purposes;
5. Ask us to erase personal data if it is no longer necessary in relation to the purposes for which it was collected or processed or to rectify inaccurate data or to complete incomplete data;
6. Restrict processing in specific circumstances;
7. Prevent processing that is likely to cause damage or distress to the data subject or anyone else;

8. Be notified of a personal data breach which is likely to result in high risk to their rights and freedoms;
9. In limited circumstances, receive or ask for their personal data to be transferred to a third party in a structured, commonly used and machine-readable format.

If any request is made to exercise the rights above, it is a requirement for the relevant staff member within Corn Close Care Farm to verify the identity of the individual making the request.

Subject Access Requests

A Data Subject has the right to be informed by Corn Close Care Farm of the following: -

1. Confirmation that their data is being processed;
2. Access to their personal data;
3. A description of the information that is being processed;
4. The purpose for which the information is being processed;
5. The recipients/class of recipients to whom that information is or may be disclosed;
6. Details of the provision's sources of information obtained;

Any Data Subject who wishes to obtain the above information must notify Corn Close Care Farm in writing of his or her request. This is known as a Data Subject Access Request. The request should in the first instance be sent to the Manager.

Employee Obligations

Employees may have access to the personal data of other members of staff, suppliers, parents/carers or visitors of Corn Close Care Farm in the course of their employment or engagement. If so, Corn Close Care Farm expects those employees to help meet the provision's data protection obligations to those individuals. Specifically, you must: -

- Only access the personal data that you have authority to access, and only for authorised purposes;
- Only allow others to access personal data if they have appropriate authorisation;
- Keep personal data secure
- Not remove personal data or devices containing personal data from the premises unless appropriate security measures are in place to secure the information;
- Not store personal information on local drives.

ACCOUNTABILITY

Corn Close Care Farm will ensure compliance with data protection principles by implementing appropriate technical and organisational measures. We are responsible for and demonstrate accountability with the GDPR principles.

Personal Data Breaches

The GDPR requires Corn Close Care Farm to notify any applicable personal data breach to the Information Commissioner's Office (ICO).

(0303 123 1113 or contact via [live chat](#). Normal opening hours are Monday to Friday between 9am and 5pm (excluding bank holidays. ico.org.uk/global)

Any suspected personal data breach should be reported to the manager, who will notify data subjects or any applicable regulator where we are legally required to do so.

If you know or suspect that a personal data breach has occurred, do not attempt to investigate the matter yourself. Immediately contact the Manager.

Transparency and Privacy Notices

Whenever we collect personal data directly from data subjects, we will provide the data subject with all the information required by the GDPR.

When personal data is collected indirectly (for example from a third party or publicly available source), we will provide the data subject with the above information as soon as possible after receiving the data. Corn Close Care Farm will also confirm whether that third party has collected and processed data in accordance with the GDPR. Notifications shall be in accordance with ICO guidance and, where relevant, be written in a form understandable by those defined as “children” under the GDPR.

Privacy by Design

Privacy by design is an approach that promotes privacy and data protection compliance from the start. To help us achieve this, Corn Close Care Farm takes into account the nature and purposes of the processing, any cost of implementation and any risks to rights and freedoms of data subjects when implementing data processes.

Record Keeping

Corn Close Care Farm are required to keep full and accurate records of our data processing activities. These records include: -

- The name and contact details of the provision;
- The contact details of the Data Protection Officer;
- Descriptions of the types of personal data used;
- Description of the data subjects;
- Details of the processing activities and purposes;
- Details of any third party recipients of the personal data;
- Where personal data is stored;
- Retention periods;
- Security measures in place.

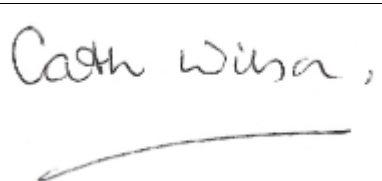
(See appendix to this policy)

Training

Corn Close Care Farm will ensure all relevant personnel have undergone adequate training to enable them to comply with data privacy laws.

Monitoring

We will regularly monitor the effectiveness of this policy and our GDPR procedures and conduct a full review annually, or in the case of a change of legislation, and the policy will be updated as appropriate.

Date of policy	22.08.22
Review date	21.08.23
Name	Cath Wilson
Signed	
Position	Manger

Appendix 1

Record Keeping Procedures:

The name and contact details of the provision;

Corn Close Care Farm
Grange Lane
Off Low Wath Road
Pateley Bridge
HARROGATE
HG3 5HL

cornclosecarefarm@btinternet.com

The contact details of the Data Protection Officer;

Cath Wilson – cornclosecarefarm@btinternet.com

Descriptions of the types of personal data used;

Name; address; date of birth; any medical conditions relevant to time at CCCF; any allergies relevant to time at CCCF; any behavioural issues relevant to time at CCCF; any identified Special Educational Need relevant to CCCF; emergency phone contacts.

Description of the data subjects;

Staff; volunteers; visitors; parents and carers.

Details of the processing activities and purposes;

Only necessary data is collected and processed. Data collected relates to information necessary to ensure safety and well-being of visitors; communication with parents/carers/schools; payment of invoices; bookings and allocating visitors to groups.

Details of any third party recipients of the personal data;

No data is shared with third parties.

Where personal data is stored;

Electronically on computer; hard copy in manual filing system.

Retention periods;

Data is kept according to:

Article 5(1)(e) says:

“1. Personal data shall be:

(e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ('storage limitation')”

Management Team			
Basic file description	Data Protection Issues	Retention Period [Operational]	Action at the end of the administrative life of the record
Records created by the Management Team	There may be data protection issues if the records refer to individual pupils or members of staff	Current academic year + 6 years then review	SECURE DISPOSAL
Correspondence created by the Management Team	There may be data protection issues if the correspondence refers to individual pupils or members of staff	Date of correspondence + 3 years then review	SECURE DISPOSAL

Registration			
Basic file description	Data Protection Issues	Retention Period [Operational]	Action at the end of the administrative life of the record
Registration Form	Yes	Date of registration + 1 year	SECURE DISPOSAL

Administration			
Basic file description	Data Protection Issues	Retention Period [Operational]	Action at the end of the administrative life of the record
General file	No	Current year + 5	SECURE DISPOSAL

series		years then REVIEW	
Records relating to the creation and publication of the brochure or other promotional material	No	Current year + 3 years	STANDARD DISPOSAL
Records relating to the creation and distribution of circulars to staff, parents/carers or visitors	No	Current year + 1 year	STANDARD DISPOSAL
Newsletters and other items with a short operational use	No	Current year + 1 year	STANDARD DISPOSAL

Staffing and Recruitment (including volunteers)			
Basic file description	Data Protection Issues	Retention Period [Operational]	Action at the end of the administrative life of the record
All records leading up to the appointment of a new member of staff – unsuccessful candidates	Yes	Date of appointment of successful candidate + 6 months	SECURE DISPOSAL
All records leading up to the appointment of a new member of staff – successful candidate	Yes	All the relevant information should be added to the staff personal file (see below) and all other information retained for 6 months	SECURE DISPOSAL
Pre-employment vetting information – DBS Checks	No	The school does not have to keep copies of DBS certificates. If the school does so the copy must NOT be retained for more than 6 months	
Proofs of identity collected as part of the process of checking “portable” enhanced DBS disclosure	Yes	Where possible these should be checked and a note kept of what was seen and what has been checked. If it is felt necessary to keep copy documentation then this should be placed on the member of staff's personal file	
Pre-employment	Yes	Where possible these documents	

vetting information – Evidence proving the right to work in the United Kingdom		should be added to the Staff Personal File, but if they are kept separately then the Home Office requires that the documents are kept for termination of Employment plus not less than two years	
--	--	--	--

Management of Disciplinary and Grievance Procedures

Basic file description	Data Protection Issues	Retention Period [Operational]	Action at the end of the administrative life of the record
Allegation of a child protection nature against a member of staff including where the allegation is unfounded ⁵	Yes	Until the person's normal retirement age or 10 years from the date of the allegation whichever is the longer then REVIEW. Note allegations that are found to be malicious should be removed from personnel files. If found they are to be kept on the file and a copy provided to the person concerned	SECURE DISPOSAL These records must be shredded
Disciplinary Proceedings	Yes		
oral warning		Date of warning + 6 months	SECURE DISPOSAL [If warnings are placed on personal files then they must be weeded from the file]
written warning – level 1		Date of warning + 6 months	
written warning – level 2		Date of warning + 12 months	
final warning		Date of warning + 18 months	
case not found		If the incident is child protection related then see above otherwise dispose of at the conclusion of the case	SECURE DISPOSAL

Health and Safety			
Basic file description	Data Protection Issues	Retention Period [Operational]	Action at the end of the administrative life of the record
Health and Safety Policy Statements	No	Life of policy + 3 years	SECURE DISPOSAL
Health and Safety Risk Assessments	No	Life of risk assessment + 3 years	SECURE DISPOSAL
Records relating to accident/ injury at work	Yes	Date of incident + 12 years In the case of serious accidents a further retention period will need to be applied	SECURE DISPOSAL
Accident Reporting	Yes		
Adults		Date of the incident + 6 years	SECURE DISPOSAL
Children		DOB of the child + 25 years	SECURE DISPOSAL
Control of Substances Hazardous to Health (COSHH)	No	Current year + 40 years	SECURE DISPOSAL
Fire Precautions log books	No	Current year + 6 years	SECURE DISPOSAL

Payroll and Pensions			
Basic file description	Data Protection Issues	Retention Period [Operational]	Action at the end of the administrative life of the record
Maternity pay records	Yes	Current year + 3 years	SECURE DISPOSAL

Records held under Retirement Benefits Schemes (Information Powers) Regulations 1995	Yes	Current year + 6 years	SECURE DISPOSAL
--	-----	------------------------	-----------------

Risk Management and Insurance			
Basic file description	Data Protection Issues	Retention Period [Operational]	Action at the end of the administrative life of the record
Employer's Liability Insurance Certificate	No	Closure of the organisation + 40 years	SECURE DISPOSAL

Accounts			
Basic file description	Data Protection Issues	Retention Period [Operational]	Action at the end of the administrative life of the record
Annual Accounts	No	Current year + 6 years	STANDARD DISPOSAL
Loans and grants managed by the organisation	No	Date of last payment on the loan + 12 years then REVIEW	SECURE DISPOSAL
Invoices, receipts, order books and requisitions, delivery notices	No	Current financial year + 6 years	SECURE DISPOSAL
Records relating to the collection and banking of monies	No	Current financial year + 6 years	SECURE DISPOSAL

Basic file description	Data Protection Issues	Retention Period [Operational]	Action at the end of the administrative life of the record
Information that contributes to the pupil's Educational Record required by The Education (Pupil Information) (England) Regulations 2005	Yes		
Primary		Retain whilst the child remains at the primary school	The file should follow the pupil when he/she leaves the primary school. ¹
Secondary		Date of Birth of the pupil + 25 years	SECURE DISPOSAL
Child Protection information held on pupil file		If any records relating to child protection issues are placed on the pupil file, it should be in a sealed envelope and then retained for the same period of time as the pupil file.	SECURE DISPOSAL – these records MUST be shredded
Child protection information held in separate files		DOB of the child + 25 years then review This retention period was agreed in consultation with the Safeguarding Children Group on the understanding that the principal copy of this information will be found on the Local Authority Social Services record	SECURE DISPOSAL – these records MUST be shredded

Attendance			
Basic file description	Data Protection Issues	Retention Period [Operational]	Action at the end of the administrative life of the record
Attendance Registers	Yes	Every entry in the attendance register must be preserved for a period of three years after the date on which the entry was made.	SECURE DISPOSAL
Correspondence relating to absence		Current academic year + 2 years	SECURE DISPOSAL

Special Educational Needs			
Basic file description	Data Protection Issues	Retention Period [Operational]	Action at the end of the administrative life of the record
Special Educational Needs files, reviews and Individual Education Plans	Yes	Date of Birth of the pupil + 25 years	REVIEW NOTE: This retention period is the minimum retention period that any pupil file should be kept. Some authorities choose to keep SEN files for a longer period of time to defend themselves in a "failure to provide a sufficient education" case. There is an element of business risk analysis involved in any decision to keep the records longer than the minimum retention period and this should be documented.

Statement /EHCP maintained under section 234 of the Education Act 1990 and any amendments made to the statement	Yes	Date of birth of the pupil + 25 years [This would normally be retained on the pupil file]	SECURE DISPOSAL unless the document is subject to a legal hold
---	-----	---	--

Security measures in place.

Only necessary information is collected, retained and stored, with permission.

Records are securely stored both electronically and in hard copy and are only accessed by the manager and permitted staff/volunteers.

Information/records are anonymised wherever possible. Initials are used wherever possible.

Staff/volunteer confidentiality section in Staff Handbook.

Privacy Policy is in place and communicated to staff.