CASTLE FARM
COUNTRYSIDE CLASSROOM

GDPR/DATA PROTECTION POLICY 09/25

Review date: 09/26

Company Number 14937009 Registered in England and Wales

CASTLE FARM COUNTRYSIDE CLASSROOM (CFCC) DATA PROTECTION AND PRIVACY POLICY

1. Aims

Castle Farm CC aims to ensure that all personal data collected about staff, learners, parents, commissioning parties, visitors and other individuals is collected, stored and processed in accordance with the General Data Protection Regulation (GDPR) and the expected provisions of the Data Protection Act 2018 (DPA 2018) as set out in the Data Protection Bill.
This policy applies to all personal data, regardless of whether it is in paper or electronic format.
Castle Farm CC will ensure that it is able to evidence compliance with the DPA of 2018 and in accordance with GDPR.

2. Legislation and guidance

This policy meets the requirements of the GDPR and the expected provisions of the DPA May 2018. It is based on guidance published by the Information Commissioner's Office (ICO) on the GDPR and the ICO's code of practice for subject access requests.
It also reflects the ICO's code of practice for the use of surveillance cameras and personal information. In addition, this policy complies with regulation 5 of the Education (Pupil Information) (England) Regulations 2005, which gives parents the right of access to their child's educational record.

.

3. Roles and responsibilities

This policy applies to all staff who are employed by Castle Farm CC, and to external organisations or individuals working on our behalf.

The Directors are responsible for overseeing the implementation of this policy, monitoring our compliance with data protection law, and developing related policies and guidelines where applicable.
They will audit the GDPR compliance of Castle Farm CC as and when required and ensure staff are aware and compliant in their day to day practice.
The Directors are also the first point of contact for individuals whose data Castle Farm CC processes.
.

Staff are responsible for:

• Collecting, storing and processing any personal data in accordance with this policy, including ensuring that:

- Any personal data that staff hold is kept securely
- Personal information is not disclosed either orally or in writing, accidentally or otherwise to any unauthorised third party
- Personal information is not transferred internationally without checking first that the right safeguards are in place.

- To avoid leaving any portable or mobile ICT equipment or removable storage media in unattended vehicles. Where this is not possible, it must be locked out of sight.
- Informing Castle Farm CC of any changes to their personal data, such as a change of address
- Contacting the Directors with any questions about the operation of this policy, data protection law,

  If they have any concerns that this policy is not being followed.

  If they are unsure whether or not they have a lawful basis to use personal data in a particular way.

  If they need to rely on or capture consent, draft a privacy notice, deal with data protection rights invoked by an individual, or transfer personal data outside the European Economic Area

  If there has been a data breach

  Whenever they are engaging in a new activity that may affect the privacy rights of individuals

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

4. Data protection principles

The GDPR is based on data protection principles that our Provision must comply with.
The principles say that personal data must be:
• Processed lawfully, fairly and in a transparent manner
• Collected for specified, explicit and legitimate purposes
• Adequate, relevant and limited to what is necessary to fulfil the purposes for which it is processed
• Accurate and, where necessary, kept up to date
• Kept for no longer than is necessary for the purposes for which it is processed
• Processed in a way that ensures it is appropriately secure

This policy sets out how Castle Farm CC aims to comply with these principles.

5. Collecting personal data

Lawfulness, fairness and transparency

Castle Farm CC will only process personal data where they have one of 6 'lawful bases' (legal reasons) to do so under data protection law:
• The data needs to be processed so that Castle Farm CC can fulfil a contract with the individual, or the individual has asked the school to take specific steps before entering into a contract
• The data needs to be processed so that the Castle Farm CC 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 Castle Farm CC, 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 Castle Farm CC or a third party (provided the individual's rights and freedoms are not overridden)
• The individual (or their parent/carer/social worker/commissioning party) when appropriate in the case of a learner) has freely given clear consent
For special categories of personal data, we will also meet one of the special category conditions for processing which are set out in the GDPR and Data Protection Act 2018.

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

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.

When using consent, Castle Farm CC must be able to demonstrate that consent has been unequivocally given, not just implied. Consent cannot apply to children under 13 unless the holders of parental responsibility have provided it. Nor can consent be coerced, for example, forced consent as part of a contract.
Consent is a valid legal basis for processing of special categories of personal information.
Consent must be prominent in any privacy statement:
• freely given, specific, informed and unambiguous
• a clear affirmative action, signifying agreement to the processing of their personal information
When consent is given in the context of a statement which also concerns other matters, the request for consent needs to be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language.
When consent is provided, it must be able to be withdrawn at any time with as much ease as it was originally given. If withdrawn, the information must be erased.
The right to data portability applies in the case of contract being the legal basis.

Legitimate Interests

It is always important to demonstrate the necessity for Castle Farm CC to process personal information for its legitimate interests if relying on this legal basis.

When using legitimate interests, WF must be able to demonstrate that there are no over-riding risks to the individuals' interests, rights or freedoms.

Contract

When using contract as the legal basis, WF must be able to demonstrate that the necessity of the performance of a contract (or negotiation of a contract) with the individual, for example, employee, supplier or customer / guest.. The right to not being subject to automated decision-making, including profiling, does not apply where there is a necessity for the purposes and legal basis of a contract (or entering into a contract).
The right to data portability applies in the case of contract being the legal basis.
NB - Consent is presumed not to be freely given if it does not allow separate consent to be given if the performance of a contract, including the provision of a service, is dependent on the consent, despite such consent not being necessary for such performance.

Legal Obligation

When there is a statutory obligation, Castle Farm CC must be able to demonstrate for the specific purposes of processing personal information what that legal obligation is.

Vital Interests

When using vital interests, Castle Farm CC must be able to demonstrate that there is a necessity to process personal information in the vital interests of the individual concerned.

Public Interest

When using public interest, Castle Farm CC must be able to demonstrate that there is a need to store personal information in the interests of the public. For example, for public safety and security purposes, retaining staff information to pass to emergency services personnel given some event.

6. DBS Checks

Agreement to Castle Farm CC processing certain types of personal data is a condition of employment for staff.
This includes information about previous criminal convictions.
All members of staff and volunteers who come into contact with children or vulnerable young adults will be subject to Enhanced DBS checks. Castle Farm CC has a duty under the Children Act, Health and Social Care Act and other enactments to ensure that staff are suitable for the job. We also have a duty of care to all staff and volunteers, and must, therefore, make sure that employees and those who use Castle Farm CC facilities do not pose a threat or danger to other users.
Consent will be requested to all staff and volunteers to hold hard copy of personal

information, including, identity checks and DBS certificates for the full term of employment.

7. Medical Information
Castle Farm CC will also ask for information about particular health needs, such as allergies to particular forms of medication, or any conditions such as asthma or diabetes.
Castle Farm CC will only use the information in the protection of the health and safety of the individual.

8. Sharing personal data
We will not normally share personal data with anyone else, but may do so where:
• There is an issue with a learner/parent/carer/social worker/commissioning party that puts the safety of our staff at risk.
• We need to liaise with other agencies – we will seek consent as necessary before doing this
• If Castle Farm CC needs to use suppliers or contractors that require data to enable the care farm to provide services to our staff and learners – for example, IT companies. When doing this, we will:
o Only appoint suppliers or contractors which can provide sufficient guarantees that they comply with data protection law.
o 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.
o Only share data that the supplier or contractor needs to carry out their service, and information necessary to keep them safe while working with us.
We will also share personal data with law enforcement and government bodies where we are legally required to do so, 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 anonymised or consent has been provided.

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 learners or staff. Where we transfer personal data to a country or territory outside the European Economic Area, we will do so in accordance with data protection law.

9. Email Communication

Due to the ease with which large quantities of personal data can be accidentally or inappropriately exposed when using email staff should be particularly careful to use email in a considered manner. In particular:
• Staff should not include any personal information in the “Subject” field of email regardless of the recipient, in particular do not include child’s names or other potential identifiers.
• Staff should make it a habit to preferentially use “Bcc” rather than “Cc”, “Cc”

should only be used where it is necessary for all recipients to see replies.
• When using Distribution Lists to send emails to those outside Castle Farm CC, ensure that email addresses are not shared. Use the “Bcc” facility so that email addresses are not displayed.

10. Retention

In accordance with the principle of Data Minimisation Castle Farm CC will hold data for no longer than is necessary for the original purpose for which the data was collected. Different categories of data will be retained for different periods of time.

11. Disposal of Information

Printed information will be shredded. Any computer or portable media containing information will be securely and permanently deleted and/or physically destroyed.

12. Subject access requests and other rights of individuals

Individuals have a right to make a ‘subject access request’ to gain access to personal information that the school holds about them. This includes:
• Confirmation that their personal data is being processed
• Access to a copy of the data
• The purposes of the data processing
• The categories of personal data concerned
• Who the data has been, or will be, shared with
• How long the data will be stored for, or if this isn’t possible, the criteria used to determine this period.
• 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.
Subject access requests must be submitted in writing, either by letter or email to the Directors

. 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, they must immediately forward it to the Directors.

Learners and subject access requests
Personal data about a child belongs to that child, and not the child’s parents or carers. For a parent or carer to make a subject access request with respect to their child, the child must either be unable to understand their rights and the implications of a subject access request or have given their consent.

Children below the age of 12 are generally not regarded to be mature enough to

understand their rights and the implications of a subject access request. Therefore, most subject access requests from parents or carers of pupils at Castle Farm CC 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.

Responding to subject access requests

When responding to requests, Castle Farm CC:

- May ask the individual to provide 2 forms of identification
- May contact the individual via phone to confirm the request was made
- Will respond without delay and within 1 month of receipt of the request
- Will provide the information free of charge
- May tell the individual we will comply within 3 months of receipt of the request, where a request is complex or numerous. We will inform the individual of this within 1 month, and explain why the extension is necessary.

Castle Farm CC will not disclose information if it:

- Might cause serious harm to the physical or mental health of the learner or another individual
- Would reveal that the learner is at risk of abuse, where the disclosure of that information would not be in the learner's best interests
- Is contained in adoption or parental order records
- Is given to a court in proceedings concerning the learner.

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.

When we refuse a request, we will tell the individual why, and tell them they have the right to complain to the ICO.

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, 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, or object to the processing of it (in certain circumstances)
- Prevent use of their personal data for direct marketing
- Challenge processing which has been justified on the basis of public interest
- Request a copy of agreements under which their personal data is transferred outside of the European Economic Area
- Object to decisions based solely on automated decision making or profiling (decisions taken with no human involvement, that might negatively affect them)
- Prevent processing that is likely to cause damage or distress
- 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 have rights which apply if Castle Farm CC take decisions about them

which are based solely on automated processing (i.e. without human intervention) and which produce significant or legal effects on the individuals.
Individuals should submit any request to exercise these rights to the Directors. If staff receive such a request, they must immediately forward it to the Directors.

13. Parental (including carers) requests to see the educational record

Parents, or those with parental responsibility, have a legal right to free access to a learner's educational record (which includes most information about a learner) within 15 working days (working days being Monday to Friday) of receipt of a written request.

14. Photographs and videos

As part of Castle Farm CC activities, we may take photographs and record images of individuals within our setting.
We will obtain written consent from parents/carers/social workers/commissioning parties for photographs and videos to be taken of a learner for communication, marketing and promotional materials. We will clearly explain how the photograph and/or video will be used to both the parent/carer/social worker/commissioning parties and learner
Uses may include:
• Outside of Castle Farm CC by external agencies such as the setting's website, newspapers, advertising campaigns
• Online on our website or, in future, on 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 learner, to ensure they cannot be identified.

15. Data protection by design and default

We will put measures in place to show that we have integrated data protection into all of our data processing activities, including:
• 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 (
• 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 of our privacy measures and make sure we are compliant

16. Data security and storage of records

We will protect personal data and keep it safe from unauthorised or unlawful access, alteration, processing or disclosure, and against accidental or unlawful loss,

destruction or damage.
In particular:
• Paper-based records and portable electronic devices, such as iPad, 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, left anywhere else where there is general access.
• Where personal information needs to be taken off site, staff must sign it in and out with the Directors
• Passwords that are at least 8 characters long containing letters and numbers are used to access school computers, laptops and other electronic devices. Staff and will be reminded to change their passwords at regular intervals.
• Staff, pupils or governors who store personal information on their personal devices are expected to follow the same security procedures as for equipment owned by Castle Farm CC
• Where we need to share personal data with a third party, we carry out due diligence and take reasonable steps to ensure it is stored securely and adequately. protected

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

18. Monitoring arrangements

The Directors is responsible for monitoring and reviewing this policy.
This policy will be reviewed and updated if necessary, when the Data Protection Bill receives royal assent and becomes law (as the Data Protection Act 2018) – if any changes are made to the bill that affect our practice. Otherwise, or from then on, this policy will be reviewed every two years.

19. Actions to minimise the impact of data breaches

Castle Farm CC 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.

20. Sensitive information being disclosed via email (including safeguarding records)

• If special category data (sensitive information) is accidentally made available via email to unauthorised individuals, the sender must attempt to recall the email as soon as they become aware of the error.
• Members of staff who receive personal data sent in error must alert the sender and

the Directors as soon as they become aware of the error.
• If the sender is unavailable or cannot recall the email for any reason, the Directors will ask the ICT department to recall it.
• In any cases where the recall is unsuccessful, the Directors 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 Directors will ensure we receive a written response from all the individuals who received the data, confirming that they have complied with this request.
• The Directors 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

21. Contacts

If you have any enquiries in relation to this policy, please contact
CFCC Directors who will also act as the contact point for any subject access requests.
Further advice and information is available from the Information Commissioner's Office, www.ico.gov.uk or telephone 01625 545745

ICO Registration Reference: ZB902445

Castle Farm Countryside Classroom
Castle Farm Countryside Classroom is the
DATA controller. Our contact details are:
Castle Farm Countryside Classroom
Plot 1 and 2
Butt Lane
Burgh Castle
Great Yarmouth
Norfolk
NR31 9QF
For queries related to this notice please contact:
• office@castlefarmcc.com

Castle Farm Countryside Classroom request your consent to hold data relating to legitimate interests.
We may retain this data for up to 1 year.
If you consent to this use of your data we will retain a record of your consent.

DECLARATION OF CONSENT
I agree to my data being processed as described above. Please
tick
Signature . . . . . .
Date . . . .

You have the right to withdraw consent at any time by contacting us or our

Data Protection Officer at the email address above.
You have the qualified right to request: access to and port your data, rectification or erasure of the data, restriction of processing, to object to the processing.
You also have a right to lodge a complaint with a Supervisory Authority, for example the Information Commissioner’s Office.