Data Protection Policy

Peopleton Brook Care Farm

Policy owner and data-protection lead: Jake Payne, Business Manager

Data-rights contact: jake@peopletonbrookfarm.co.uk

Approval date: 05/08/2026

Effective date: 01/09/2026

Next review: August 2027, or sooner if law, processing or provision changes

> **Plain-language commitment:** We use the minimum personal information needed to provide safe, effective alternative provision. We explain what we do, protect information, respect the rights of children and adults, and act promptly when something goes wrong.

1. Purpose, status and scope

Peopleton Brook Care Farm (PBCF) is a non-school alternative learning provider for children and young people, including learners with special educational needs and disabilities, and also supports adult participants. This policy governs PBCF's handling of personal information in its own capacity as controller and, where a contract says so, as processor for a commissioning body.

It applies to staff, volunteers, owners, contractors, temporary workers and anyone handling information for PBCF. It covers paper and digital records, email, messaging, photographs, video, audio, CCTV where used, radio communications, online systems, portable media and information held off site or during transport, visits and outreach.

The principal framework is the UK GDPR and Data Protection Act 2018 as amended, including by the Data (Use and Access) Act 2025. The Privacy and Electronic Communications Regulations apply where relevant. Freedom of information legislation applies only where PBCF is legally within scope or holds information on behalf of a public authority; this policy does not claim public-authority status.

2. Governance and responsibilities

PBCF will document whether it and each commissioning school, academy, local authority, health body or supplier acts as controller, joint controller or processor for each material activity. Contracts and privacy information must reflect the actual decision-making relationship; labels alone do not decide legal status.

Role	Responsibility
Business Owners	Approve resources and risk controls, oversee serious incidents and complaints, and ensure independent escalation where the data-protection lead is involved.

Role	Responsibility
Data-protection lead - Jake Payne	Coordinate compliance, records of processing, privacy information, rights requests, DPIAs, contracts, breaches, complaints, training and ICO contact. This operational title does not assert that PBCF is legally required to appoint a statutory DPO.
Managers	Build privacy and security into activities, check staff access, approve sharing and escalate changes or incidents.
All workers	Use information only for authorised work, follow security rules, report errors immediately, complete training and challenge unsafe practice.
Processors and contractors	Act only on documented instructions, maintain appropriate security, assist with rights and breaches, and delete or return data as contracted.

Anyone may contact the data-protection lead. A concern about Jake Payne must be sent to an uninvolved Business Owner; nobody will investigate or decide a complaint about themselves. PBCF will obtain independent specialist advice where the risk or conflict requires it.

3. Data-protection principles and accountability

PBCF must process personal information lawfully, fairly and transparently; for specified and legitimate purposes; using only what is adequate, relevant and necessary; keeping it accurate; retaining it no longer than needed; and protecting it with appropriate technical and organisational measures. PBCF is responsible for, and must be able to demonstrate, compliance.

- maintain proportionate records of processing, lawful bases, special-category and criminal-offence conditions, sharing, processors and retention;
- issue concise, accessible and age-appropriate privacy information, including the right to complain to PBCF and the ICO;
- apply privacy by design and default and complete a data protection impact assessment (DPIA) before likely high-risk processing;
- record decisions, balancing tests, consent evidence, incidents, requests and complaints; and
- review access, security, suppliers, retention and training at planned intervals and after material change.

4. Information used and lawful bases

Depending on the service, PBCF may use identity and contact details; attendance and placement information; education, behaviour and progress records; SEND and support needs; health, disability, dietary and medication information; safeguarding and incident records; family and professional contacts; photographs or recordings; staff and volunteer employment, vetting, training and payroll records; visitor and contractor records; and system, device or security logs.

Before processing begins, PBCF will identify and record an Article 6 lawful basis. These may include contract, legal obligation, vital interests, public task where the particular function legally qualifies, consent, legitimate interests, or a recognised legitimate interest introduced by the 2025 Act. PBCF will not use public task merely because work is education-related, and it will not use consent where a person has no genuine choice.

Special-category information requires both an Article 6 basis and an Article 9 condition, supported where necessary by an appropriate policy document. Criminal-offence information requires Article 10 and Data Protection Act authority. The basis must be reassessed if the purpose changes materially.

5. Children, capacity and accessible transparency

Children merit specific protection. PBCF will put their best interests and higher protection needs at the centre of design, use plain and age-appropriate explanations, collect the minimum information, avoid unnecessary profiling, and consider the child's maturity, vulnerability, SEND, communication and decision-making ability.

Data-protection rights belong to the child as well as to adults. A child who understands the request and its consequences may exercise their own rights. A parent or carer does not automatically have a right to a child's personal information; PBCF will consider authority, the child's competence and wishes, confidentiality, safeguarding risk and the best interests of the child. Proof of parental responsibility or authority may be requested where proportionate.

For adults, capacity is decision-specific and presumed unless established otherwise. PBCF will support communication and consider lawful representatives or advocates. Disability, language, literacy or communication needs must not prevent a person receiving privacy information, making a request or raising a complaint.

6. Collecting, recording and accuracy

Staff must collect information from reliable sources, distinguish fact from professional opinion or allegation, use respectful and objective language, record the source and date where material, and correct or annotate inaccuracies promptly. Safeguarding records must preserve the original account and audit trail; a disputed professional opinion is not erased merely because the person disagrees, but the challenge and outcome should be recorded.

Information should normally be entered only into approved systems and forms. Duplicate notes, private contact lists and local downloads must be avoided. Staff must not put participant information into personal notebooks, consumer AI services, unapproved apps, personal cloud storage or personal messaging accounts.

7. Sharing and commissioning arrangements

PBCF may share information with commissioning bodies, parents or carers where lawful, local authorities, education and health professionals, emergency services, safeguarding partners, insurers, professional advisers, regulators and suppliers. Sharing must be necessary, proportionate, accurate, relevant, secure and limited to people who need it. The lawful basis, purpose, recipient and decision should be recorded for significant or unusual sharing.

> **Safeguarding and emergencies:** Data protection law does not prevent necessary and proportionate information sharing to protect a child or adult at risk. Consent is not always required. Staff must follow safeguarding procedures, share only what is needed, record the reason and never delay an urgent referral while waiting for the data-protection lead.

PBCF will tell the commissioning body promptly about attendance, welfare, safeguarding, progress and significant incidents as the placement agreement and law require. The commissioning body retains its own statutory records and decisions. PBCF must not promise to amend or delete records controlled by another organisation, but will route the request without undue delay and explain who is responsible.

8. Photographs, recordings, CCTV and communications

- Operational or safeguarding images require a documented purpose and lawful basis; promotional images normally require genuine, specific and withdrawable consent unless another basis is clearly justified.
- A person's refusal or withdrawal of promotional consent must not disadvantage their education, care or access to the service. Withdrawal affects future use and any use that can reasonably be stopped; it does not make earlier lawful processing unlawful.
- Only authorised PBCF equipment may be used. Personal phones and devices must not be used to photograph, record, store or communicate participant information.
- Two-way radios must use call signs and the minimum operational detail. Health, safeguarding, addresses and other sensitive information must move to a private authorised channel or face-to-face discussion.
- If CCTV or body-worn recording is introduced or materially changed, PBCF must complete necessity, proportionality, transparency, access, retention and DPIA checks before use.

9. Online systems, artificial intelligence and automated decisions

New systems, monitoring tools, biometric functions, generative AI or automated decision-making must not be used with personal information until authorised. Approval requires a defined purpose, lawful basis, supplier and transfer checks, security assessment, minimisation, retention controls, transparency and a DPIA where processing is likely high risk.

Staff must not enter names, case histories, images, identifiable scenarios, safeguarding information or confidential business records into public or unapproved AI tools. AI output must be treated as unverified, checked by a competent person for accuracy, bias and inappropriate disclosure, and never copied into a record without human review and an identified source.

PBCF will not make a solely automated decision producing legal or similarly significant effects unless the law permits it and required safeguards are in place. The person will receive meaningful information, a route to make representations, and human review or contest where required. Special-category data and decisions affecting children require enhanced caution and documented assessment.

10. Security, access and working practices

- use unique accounts, strong passwords and multi-factor authentication where available; never share credentials;
- apply role-based least-privilege access and remove or amend access promptly when roles change or employment ends;

- lock screens and cabinets, use approved encryption and secure transfer methods, and keep clear desks in shared areas;
- verify recipients, attachments and permissions before sending; use blind copy only where appropriate and check mailing lists;
- keep paper and devices secure during transport; do not leave records visible in vehicles or public places;
- install updates, maintain backups and test recovery proportionately; and
- dispose of paper through confidential destruction and securely erase or destroy electronic media before reuse or disposal.

Remote working must use approved equipment and systems unless specifically authorised after risk assessment. Private household members must not see or hear confidential information. Suspected phishing, malware, lost equipment or unauthorised access must be reported immediately.

11. Retention, deletion and legal holds

PBCF will maintain a retention schedule based on purpose, legal and contractual duties, limitation periods, safeguarding value and sector guidance. It will not claim that one external schedule automatically fixes every retention period. Owners of record sets must review and securely dispose of information when the period ends.

Deletion must be suspended where information is needed for a safeguarding review, complaint, rights request, investigation, insurance matter, litigation or regulatory hold. Backups may be retained for limited recovery cycles with access restrictions. Anonymisation must make re-identification not reasonably likely; pseudonymised information remains personal data.

12. Individual rights and requests

Depending on the circumstances, people have rights to be informed, access their information, rectify inaccurate information, erase information, restrict processing, receive portable information, object, and obtain safeguards around automated decisions. Rights are not absolute and PBCF will explain any lawful restriction or refusal.

Requests may be verbal or written and do not need special wording. Any worker receiving a request must record the date and send it to the data-protection lead immediately. PBCF will verify identity only to the extent reasonable and proportionate, clarify scope where genuinely needed, and normally respond without undue delay and within one month. A lawful extension of up to two further months may apply for complexity or number, with notice within the first month.

For access requests, PBCF will make reasonable and proportionate searches, consider third-party information and exemptions carefully, keep an audit trail, and provide information securely in an accessible form. The response period may be paused where legislation permits while necessary clarification or identity information is awaited; PBCF will not use clarification to delay a clear request.

13. Personal-data breaches

A personal-data breach includes accidental or unlawful loss, destruction, alteration, unauthorised disclosure of, or access to personal information. Examples include misdirected email, lost paper or equipment, inappropriate conversation, excessive system permissions, malware, unauthorised photography and information entered into an unapproved AI tool.

- Contain immediate risk without destroying evidence: recall or restrict access where safe, recover material, disconnect compromised equipment if instructed, and preserve logs.
- Report immediately to the data-protection lead and manager. Include what happened, when, information and people affected, recipients, current access and action taken.
- Record every breach and assess likelihood and severity of risk to people's rights and freedoms, including safeguarding, discrimination, identity, financial, reputational and confidentiality harms.
- Notify the ICO without undue delay and, where feasible, within 72 hours of awareness when the legal risk threshold is met. Delay must be explained; a processor must notify the controller without undue delay.
- Tell affected people without undue delay when the breach is likely to result in a high risk, using clear advice on protective action, unless a lawful exception applies.
- Notify commissioners, insurers, safeguarding bodies, police or suppliers where contract, law or risk requires, and complete lessons and corrective actions.

14. Data-protection complaints

A complaint may concern collection, access, accuracy, disclosure, security, retention, deletion, direct marketing, monitoring or any other use of personal information. It can be made verbally or in writing to any worker and does not need to cite data-protection law. PBCF will provide reasonable adjustments and may accept an authorised representative.

For complaints received on or after 19 June 2026, PBCF will acknowledge receipt within 30 days; take appropriate steps, including proportionate enquiries, without undue delay; keep the complainant informed; and tell them the outcome without undue delay. The outcome will explain findings, action, unresolved points and the right to complain to the Information Commissioner's Office at ico.org.uk/make-a-complaint or 0303 123 1113.

A complaint may also reveal a breach, safeguarding concern or rights request. Each route must be opened and handled in parallel where needed. Complaint records will be kept securely and conflicts of interest managed under the Complaints and Concerns Procedure.

15. International transfers and suppliers

PBCF will identify where suppliers store or remotely access personal information. A restricted transfer outside the UK may occur only where an adequacy regulation, appropriate safeguards such as the UK International Data Transfer Agreement or approved addendum, or a lawful exception applies, together with any required transfer risk assessment and supplementary measures.

Processor contracts must include required Article 28 terms, confidentiality, security, sub-processor controls, assistance with rights, breaches and DPIAs, deletion or return, and audit information. PBCF will perform proportionate due diligence before appointment and review suppliers according to risk.

16. Training, monitoring and non-compliance

Workers will receive data-protection and information-security instruction at induction, at least annually, and when roles, systems or law change. Higher-risk roles receive additional training. Completion and understanding will be recorded, and simulated or practical checks used where proportionate.

PBCF will monitor requests, complaints, breaches, access, retention, supplier issues, training and recurring errors. Deliberate, reckless or repeated failure may lead to removal of access, supervision, disciplinary or contractual action, safeguarding referral, regulatory notification or reporting to police where appropriate. Good-faith incident reporting will be encouraged.

Appendix A - Staff quick response

Situation	Immediate action
A person asks for their information	Record the date and exact request; verify contact details; send it to Jake Payne immediately. Do not insist on a form or written request.
Information is sent or shown to the wrong person	Contain if safe, do not conceal it, preserve evidence and report immediately. Do not decide alone whether ICO notification is needed.
Safeguarding information needs sharing	Follow safeguarding procedure and share necessary, proportionate information promptly; record what, with whom and why.
A parent requests a child's record	Do not disclose automatically. Refer for competence, authority, confidentiality, best-interests and safeguarding checks.
A new app, AI tool, camera or monitoring system is proposed	Do not upload or collect personal information until purpose, lawful basis, contract, security, transparency and DPIA needs are approved.
A caller asks for information	Verify identity and authority using trusted contact details; call back through a known number if necessary; disclose only the minimum or refer the request.
A person complains about data handling	Listen and record; route it immediately as a data-protection complaint and screen separately for breach, safeguarding and rights-request action.

Appendix B - Minimum compliance records

- record of processing, controller/processor mapping, lawful bases, Article 9/10 conditions and balancing tests;
- privacy-notice versions, consent records, withdrawal actions and appropriate-policy documentation;
- DPIAs, system approvals, supplier due diligence, contracts and international-transfer records;
- rights-request and complaint logs, including identity, searches, disclosures, exemptions, enquiries, outcomes and deadlines;
- breach log, risk assessment, notifications, communications and corrective action; and
- retention schedule, disposal evidence, legal holds, training, access reviews and audit actions.

Sources and related guidance

UK General Data Protection Regulation and Data Protection Act 2018, as amended — UK Parliament.

Data (Use and Access) Act 2025 and 2026 commencement regulations — UK Parliament.

Data Protection in Schools (updated 9 July 2026) — Department for Education.

Children and the UK GDPR (updated May 2026) — Information Commissioner's Office.

How to Deal with Data Protection Complaints (2026) — Information Commissioner's Office.

Personal Data Breaches; Individual Rights; Security; DPIAs; International Transfers — Information Commissioner's Office.

Information Sharing: Advice for Practitioners Providing Safeguarding Services — HM Government.

Approval record

Approving authority	Name	Signature	Date
Business Owner / authorised approver	Jake Payne	Jake Payne	05/08/2026