

PACE Education Pathways

Data Protection and UK GDPR Policy

ICO Ref: ZC193549

Document control

Document control	Detail
Policy title	Data Protection and UK GDPR Policy
Version	3.0
Status	Approved for use
Policy owner	Nathan Warr – Operations / Governance Lead
Approved by	Nathan Warr
Applies to	Directors, employees, tutors, associate tutors, subcontractors, volunteers and any person processing personal data for or on behalf of PACE Education Pathways
Date approved	21/08/2026
Next review date	12 months from approval, or earlier where a review trigger applies
Review trigger	Earlier review if data protection law or ICO guidance changes; PACE introduces or materially changes systems, processors or service delivery; a significant data breach or complaint occurs; safeguarding or commissioner requirements change; or an audit identifies a control weakness.
Linked documents	Privacy Notice; Records Retention Schedule; Data Breach Log; Parent / Carer Consent and Information Sharing Form; Safeguarding and Child Protection Policy; Online Safety and Acceptable Use Policy; Staff Code of Conduct and Low-Level Concerns Policy; Single Central Record; Workforce Competency and Compliance Register; safeguarding, attendance, incident and risk-assessment records.

Governance note

PACE Education Pathways treats data protection as part of safeguarding, professional practice and organisational accountability. Personal information must be processed lawfully, fairly, transparently and securely. Data protection must not be used as a reason to withhold information where sharing is lawful, necessary and proportionate to protect a child or another person from harm.

1. Purpose

PACE processes personal data about pupils, parents and carers, staff, tutors, commissioners, applicants, suppliers and professional contacts. This may include sensitive education, safeguarding, SEND, health, behaviour, attendance, family and workforce information. This policy sets out the controls PACE uses to protect that information and demonstrate compliance with UK data-protection requirements.

2. Scope

This policy applies to personal data held or used in any format, including paper records, email, approved cloud systems, safeguarding and attendance systems, HR and recruitment records, finance records, websites, messaging, online learning platforms and information exchanged with commissioners or statutory agencies. It applies throughout the information lifecycle from collection to secure disposal.

3. Legal and guidance framework

- UK General Data Protection Regulation (UK GDPR).
- Data Protection Act 2018.
- Privacy and Electronic Communications Regulations where relevant.
- Current Information Commissioner's Office (ICO) guidance on accountability, security, data breaches, individual rights and children's information.
- Current safeguarding information-sharing requirements, including Keeping Children Safe in Education and Working Together to Safeguard Children.

4. Data protection principles

- Lawfulness, fairness and transparency.
- Purpose limitation.
- Data minimisation.
- Accuracy.
- Storage limitation.
- Integrity and confidentiality (security).
- Accountability: PACE must be able to demonstrate how these principles are applied.

5. Roles and responsibilities

Role	Responsibility
Operations / Governance Lead	Owns this policy; maintains data-protection arrangements, breach oversight, records of processing and retention controls; coordinates responses to rights requests and ICO matters; and monitors compliance.
DSL / Education Lead	Ensures safeguarding information is recorded, accessed and shared lawfully and proportionately, and that data-protection considerations do not delay necessary safeguarding action.
All staff and tutors	Use approved systems, access only information needed for their role, maintain confidentiality, report breaches or misdirected information immediately, and complete required training.
Suppliers / processors	Process information only under agreed instructions and contractual safeguards, with appropriate security and confidentiality controls.

6. Information PACE processes

Category	Examples
Pupil information	Identity, contact, education history, referral details, attendance, engagement, learning and progress.
Special-category / sensitive information	SEND, disability, medical needs, wellbeing, safeguarding, risk, family context and equality information where relevant.
Parent / carer information	Contact details, consent, communications, emergency information and information relevant to provision or safeguarding.
Workforce information	Recruitment, identity and right-to-work checks, DBS/suitability status, references, qualifications, training, supervision, payroll and emergency contacts.
Commissioner / professional information	School and local-authority contacts, referrals, contracts, reports, meeting notes and professional communications.

7. Lawful basis and special-category data

PACE will identify and document an appropriate lawful basis before processing personal data. Depending on the context, this may include contract, legal obligation, legitimate interests, public task where applicable to a commissioned arrangement, vital interests in an emergency, or consent where consent is genuinely appropriate and freely given.

Where special-category or criminal-offence data is processed, PACE will identify the additional legal condition required by the UK GDPR and Data Protection Act 2018. Safeguarding, health, SEND and staff-suitability information will only be used where necessary and proportionate for the relevant purpose.

8. Collection, transparency and data minimisation

- Provide appropriate privacy information when personal data is collected or as otherwise required.
- Collect only information reasonably required for provision, safeguarding, employment, legal, contractual or governance purposes.
- Avoid collecting speculative, excessive or irrelevant personal information.
- Keep records factual and distinguish observation, reported information and professional judgement where relevant.
- Review forms, systems and data fields periodically to ensure continuing necessity.

9. Information sharing and safeguarding

Information will be shared only where there is a lawful basis and the sharing is necessary, relevant and proportionate. Safeguarding information may be shared without consent where this is required to protect a child or another person, support statutory safeguarding functions, prevent or detect crime, or where another lawful basis applies. Staff must not delay urgent safeguarding action because they are uncertain about data protection; advice should be sought from the DSL or Governance Lead as soon as practicable.

- Record significant information-sharing decisions and the rationale where appropriate.
- Share the minimum information necessary for the purpose.
- Use secure channels for sensitive information wherever practicable.
- Check recipients carefully before sending information.
- Follow commissioner information-sharing arrangements where these are lawful and do not reduce PACE safeguarding standards.

10. Security and access controls

- Use approved, access-controlled systems for pupil, safeguarding, workforce and business records.
- Apply strong passwords and multi-factor authentication where available.
- Restrict access according to role and need-to-know.
- Keep devices, screens and paper records secure from unauthorised access.
- Do not store identifiable pupil or safeguarding information in personal cloud accounts or unapproved apps.
- Avoid local downloads or printing unless necessary; dispose of paper and electronic records securely.
- Report lost devices, compromised accounts, suspicious messages, accidental disclosures and other security concerns immediately.

11. Approved systems, processors and new technology

PACE will maintain oversight of the systems and suppliers used to process personal data. Before adopting a new system or processor, PACE will consider the purpose, categories of data, access, storage, security, contractual safeguards, retention, deletion, data location and any commissioner requirements.

Where processing is likely to result in a high risk to individuals, or involves significant new technology or systematic sensitive-data processing, PACE will consider whether a Data Protection Impact Assessment (DPIA) is required before implementation.

12. Individual rights

Individuals may have rights of access, rectification, erasure, restriction, portability, objection and rights relating to automated decision-making, depending on the legal basis and circumstances. Requests must be forwarded promptly to the Operations / Governance Lead. PACE will verify identity where necessary and respond within applicable statutory timescales.

Safeguarding, third-party, legal-privilege or other exemptions may affect what can lawfully be disclosed. Records must not be altered, deleted or concealed because a rights request has been received.

13. Data breaches

A personal data breach includes accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data. All suspected breaches must be reported to the Operations / Governance Lead immediately and recorded in the Data Breach Log.

- Contain the breach and protect affected information where possible.
- Establish what happened, when, what data is affected and whose data is involved.
- Assess the likely risk to individuals.
- Consider notification to the ICO where legally required; where notification is required it must be made without undue delay and, where feasible, within 72 hours of becoming aware of the breach.
- Inform affected individuals where legally required because of high risk.
- Record the decision, rationale, corrective actions and lessons learned.

14. Accuracy, retention and secure disposal

PACE will take reasonable steps to keep personal data accurate and current. Records will be retained only for as long as justified by safeguarding, education, employment, legal, contractual, insurance, finance, audit and commissioner requirements. The Records Retention Schedule will define operational retention periods. When retention is no longer justified, information will be securely deleted, destroyed or anonymised.

15. Remote working, email and portable devices

- Use PACE-approved accounts and systems for work wherever possible.
- Do not leave devices or papers visible or accessible to unauthorised people.
- Check email addresses, attachments and permissions before sending.
- Use secure sharing rather than ordinary email attachments for highly sensitive information where practical.
- Avoid discussing identifiable pupil or staff matters where conversations can be overheard.
- Follow the Online Safety and Acceptable Use Policy when delivering remote learning or using digital platforms.

16. Training, monitoring and assurance

All staff and tutors must receive data-protection induction appropriate to their role and periodic refresher guidance. The Governance Lead will review breaches, complaints, rights requests, processor arrangements, access controls, training completion, retention and audit findings to identify patterns and required improvements.

17. Concerns, complaints and ICO

Questions or concerns about PACE data handling should be raised with the Operations / Governance Lead. PACE will investigate concerns proportionately and seek to resolve them transparently. Individuals also have the right to raise concerns with the Information Commissioner's Office. The related Privacy Notice will identify PACE contact and registration information for external transparency.

18. Review

This policy will be reviewed at least annually and earlier when a review trigger in the document-control table applies. Review will consider legal and ICO guidance changes, safeguarding requirements, new systems or suppliers, incidents and breaches, commissioner requirements and lessons from audits or complaints.

Appendix A — Data breach first-response checklist

- What happened and when?
- What personal data is involved?
- Whose information is affected?
- Has the breach been contained?
- Could any data still be accessed, recalled, deleted or secured?
- What is the likely impact on the individuals affected?
- Does the ICO need to be notified?
- Do affected individuals need to be informed?
- Do safeguarding, commissioner, insurer or other notifications apply?
- What corrective action and learning are required?

Appendix B — Minimum accountability records

Record	Purpose
Privacy Notice	Explains externally how PACE uses personal information.
Records Retention Schedule	Defines how long categories of records are retained.
Data Breach Log	Records breaches, risk assessment, notifications and actions.
Information-sharing / safeguarding records	Evidence significant sharing decisions and safeguarding rationale where appropriate.
Processor / system records	Evidence oversight of suppliers and systems processing personal data.
Training / compliance records	Evidence staff awareness and competence.