

Proactive Young People CIC

Data Protection Policy

1. Purpose and scope

Proactive Young People CIC ("PYP CIC", "we", "us") respects the privacy of the children and young people who take part in our programmes, their parents and carers, the schools, colleges and employers we work with, and our staff, volunteers and placement students. Our aim is that everyone who uses or works with PYP CIC can be confident their personal data is handled lawfully, fairly, transparently and securely.

This policy applies to all personal data we process, in any format (electronic, paper, photographs, video and audio), and to everyone who works for or on behalf of PYP CIC, including directors, employees, sessional staff, volunteers, contractors and students on placement.

2. Legal framework

We comply with:

- the **UK General Data Protection Regulation (UK GDPR)** and the **Data Protection Act 2018**, both as amended by the **Data (Use and Access) Act 2025**;
- the **Privacy and Electronic Communications Regulations 2003 (PECR)**, for email/text marketing and website cookies.

We also have regard to relevant guidance, including ICO guidance, *Keeping Children Safe in Education* (current edition) where we work in or on behalf of schools and colleges, *Working Together to Safeguard Children* (2026) and the Government's *Information sharing advice for practitioners providing safeguarding services*.

The UK data protection regulator is referred to in this policy as the ICO. From 30 September 2026, under the Data (Use and Access) Act 2025, the Information Commissioner's Office becomes the Information Commission; it continues to be known as the ICO.

3. Roles and responsibilities

- **Directors** are accountable for PYP CIC's compliance with data protection law.
- **Data Protection Lead:** Nicholas Brosnan (CEO), nicholas@proactiveyoungpeoplecic.co.uk. The Lead maintains our records of processing and retention schedule, oversees data protection impact assessments (DPIAs), manages breaches, subject access requests and data protection complaints, liaises with the ICO, and keeps this policy under review. PYP CIC has not appointed a statutory Data Protection Officer (DPO); the Lead records and reviews the assessment of whether a DPO is required as our activities change. Nicholas Brosnan is the contact for data protection matters.
- **Designated Safeguarding Lead (DSL):** Samantha Fitzgerald, samantha@proactiveyoungpeoplecic.co.uk. The DSL manages safeguarding-related information sharing in line with our Safeguarding and Child Protection Policy and, when working for a school, the school's instructions and safeguarding arrangements.
- **All staff, volunteers and placement students** must follow this policy, complete data protection training, and report any actual or suspected data breach to the Data Protection Lead immediately.

4. Data protection principles

We will ensure that personal data is:

- processed lawfully, fairly and transparently;
- collected for specified, explicit and legitimate purposes and not used in ways incompatible with those purposes;
- adequate, relevant and limited to what is necessary;
- accurate and, where necessary, kept up to date;
- kept no longer than necessary; and
- kept secure, using appropriate technical and organisational measures.

We are responsible for, and must be able to demonstrate, compliance with these principles (accountability). We do this through our records of processing (our **personal data matrix**), privacy notices, DPIAs, training records, contracts with processors and our breach log.

5. Information we hold and why

Full details of the personal data we hold are recorded in our personal data matrix, which is reviewed at least annually. We collect only the information we need, and we provide privacy notices explaining what we collect, why, who we share it with and how long we keep it. We have separate, age-appropriate privacy information for young people.

Controller or processor? We assess our role for each processing activity and document it in our personal data matrix and relevant agreements. Where PYP CIC decides why and how personal data is used, we are a controller (or, where we jointly decide this with another organisation, a joint controller). Where we process personal data only on behalf of a school, college or other organisation, we are a processor and follow its documented instructions under a written Article 28 agreement, including instructions on access, sharing, retention, return or deletion, unless the law requires otherwise. We promptly refer requests and safeguarding concerns to the appropriate school contact, subject to any urgent safeguarding duty, and tell the organisation without undue delay about a personal data breach affecting data we process on its behalf. We identify any separate processing for our own purposes and our corresponding responsibilities.

Who	Examples of data	Lawful basis (UK GDPR Art. 6)	Special category / criminal offence data
Young people on our programmes	Name, school, year group, contact details, emergency contacts, attendance, placement details, career interests and outcomes, incident/accident records	Where PYP CIC is a controller: the basis is recorded by purpose in our personal data matrix and privacy notice; legitimate interests (Art. 6(1)(f)) may apply to necessary programme delivery after an assessment. Necessary safeguarding may use recognised legitimate interest (Art. 6(1)(ea), Annex 1) where its conditions are met, or another appropriate basis. Where we act only as processor, the school or other controller determines its lawful basis.	For health or other special category information, record a suitable Art. 9 condition for each purpose. Explicit consent (Art. 9(2)(a)) may apply where freely given; safeguarding may use Art. 9(2)(g) with DPA 2018 Sch. 1 para. 18 only where its conditions are met. Vital interests (Art. 9(2)(c)) may apply in a relevant emergency. Criminal offence information requires a separate Art. 10 condition. Document any required Appropriate Policy Document.
Parents / carers	Name, contact details, relationship to young person, consents given	Legitimate interests; consent where we rely on it (e.g. photos).	Not normally collected.
School, college and employer contacts; placement providers	Names, job titles, work contact details, placement risk-assessment information	Legitimate interests for ordinary business contacts where appropriate; contract (Art. 6(1)(b)) only where the individual is personally party to the contract. Record the basis by purpose in the personal data matrix.	Not normally collected.

Who	Examples of data	Lawful basis (UK GDPR Art. 6)	Special category / criminal offence data
Staff, volunteers and placement students	Recruitment records, right-to-work, contract, payroll, HMRC, pension, training, supervision, performance	Contract; legal obligation.	Health (such as sickness or adjustments): Art. 9(2)(b) and DPA 2018 Sch. 1 para. 1 where its conditions apply. DBS/criminal offence data: Art. 10 and a documented DPA 2018 Sch. 1 condition appropriate to the particular check. Maintain an Appropriate Policy Document where required.
Photographs, video and case studies	Images and quotes used in reports or publicity	Consent for specified optional uses, obtained from a young person with sufficient understanding or a person with parental responsibility where appropriate. Record the permitted channels and duration; explain withdrawal and stop future use following withdrawal.	–
Marketing and newsletters	Name, email address	Record the UK GDPR basis and applicable PECR rule by campaign and recipient type. Obtain consent where required; use a soft opt-in only where its precise conditions are met. Identify PYP and offer a clear opt-out in each message.	–

Where a condition in Schedule 1 of the Data Protection Act 2018 requires an Appropriate Policy Document, we maintain one alongside our other data protection documents.

6. Confidentiality

Within PYP CIC we respect confidentiality in the following ways:

- We only share information about a young person with their own parent/carer where this is appropriate, taking account of the young person's age, maturity and wishes (see section 7).
- Information given to us by young people, parents or carers is passed to third parties only where we have a lawful basis, as explained in our privacy notices, including where there is a safeguarding concern (see our **Safeguarding Policy**).
- Safeguarding concerns and records are kept in a secure, restricted-access file, accessible only to the DSL, the Data Protection Lead and those who need to know.
- Staff discuss individual young people only for legitimate purposes such as planning, delivery, safeguarding and group management.
- Staff employment matters remain confidential to those making personnel decisions.
- Staff, volunteers and placement students are made aware of confidentiality and this policy during induction and are required to respect it.

7. Children and young people

Children and young people have data protection rights in their own right. In England, we assess a young person's ability to understand and exercise a right individually, taking account of their age, maturity, understanding and the nature of the information; we do not apply a fixed age threshold. Where a young person understands the request, we will usually deal directly with them and consider their views before disclosing their information to a parent or carer. A parent or carer may act for a young person where they

are not competent to act themselves or have authorised the parent or carer to act, subject to safeguarding and the young person's best interests. We write privacy information in clear, age-appropriate language. Any specific age rule for consent to a directly offered online service is considered separately if applicable.

8. Sharing information with third parties

- We share personal data only where it is necessary, proportionate and lawful, and only the minimum information needed (for example, a placement provider receives only what it needs to host a young person safely).
- Where we rely on consent to share or use personal data, we record what the person agreed to and provide an easy way to withdraw it. We seek consent from a young person who can understand the particular use, or from a person with parental responsibility where the young person cannot, unless this would be contrary to the young person's best interests. We treat participation in a programme separately from optional use of images, quotes or case studies. Where sharing is based on another lawful basis, we explain that in our privacy notices.
- **Safeguarding:** data protection law does not prevent the sharing of information to keep children safe. Where there is a safeguarding concern, the DSL may share information with children's social care, the police or other agencies without consent where that is necessary and proportionate. We record what was shared, with whom, when and why.
- We share information with legally authorised bodies (e.g. police, HMRC, courts) where the law requires or permits it.
- We only use suppliers that process personal data on our behalf (e.g. IT, cloud storage, payroll) under a written contract meeting UK GDPR Article 28, and check that any transfer of data outside the UK is lawful.

9. Keeping data secure

- Electronic records are held in approved, access-controlled systems; access is limited by role and removed promptly when someone leaves.
- Accounts use strong passwords and multi-factor authentication; laptops and phones are encrypted, screen-locked and kept up to date.
- Personal data must be held and transferred only through approved systems. It must not be stored on personal devices, personal email accounts or unencrypted USB drives. Any exception involving a personal device must be assessed and authorised in advance by the Data Protection Lead, with appropriate security controls, including encryption and access restrictions.
- Paper records are kept in locked storage, not left unattended, and securely shredded when no longer needed.
- Emails containing sensitive personal data are sent securely and checked for the correct recipient before sending.

10. New technology, AI and DPIAs

- We screen proposed new processing for privacy risks and carry out a data protection impact assessment (DPIA) before processing likely to result in a high risk to individuals. This includes assessing new technology and processing involving children or special category data against the ICO criteria. We record the screening decision and the DPIA where required.
- Staff must not enter personal data about young people, parents or staff into generative AI tools or other online services unless the tool has been approved by the Data Protection Lead and appropriate safeguards are in place.
- We do not make decisions about individuals based solely on automated processing that have legal or similarly significant effects on them.

11. Retention and disposal

We retain each category of record for the period in our retention schedule, with a documented reason. Routine programme and placement administration records, safeguarding records, accident and incident records, records needed for potential claims, personnel, payroll and tax records may require different periods. The Lead reviews periods in light of legal requirements, contractual terms, insurance requirements and the rights of children and young people. We securely delete or destroy records when their period expires. Where

we act as a processor for a school or another organisation, we follow its documented return or deletion instructions under the agreement, unless the law requires otherwise. We suspend routine deletion where a complaint, claim, investigation or safeguarding need requires preservation.

12. Data breaches

A personal data breach is any security incident leading to the accidental or unlawful loss, destruction, alteration, unauthorised disclosure of, or access to, personal data (for example, an email sent to the wrong person or a lost laptop).

- All suspected breaches must be reported to the Data Protection Lead immediately.
- Every breach is recorded in our breach log, including the facts, effects and action taken.
- Where we process personal data on behalf of a school, college or other organisation, we tell that organisation without undue delay after becoming aware of a breach affecting its data, so that it can decide whether to report it.
- If a breach is likely to result in a risk to people's rights and freedoms, we report it to the ICO without undue delay and, where feasible, within **72 hours** of becoming aware of it.
- If a breach is likely to result in a high risk, we also tell the individuals affected without undue delay.

13. Individuals' rights

Individuals have the right to: be informed; access their personal data; rectification; erasure; restrict processing; data portability; object to processing; and rights relating to automated decision-making. Where we rely on consent, it can be withdrawn at any time.

Subject access requests (SARs)

- Young people, parents/carers (see section 7), staff, volunteers and others can ask for a copy of the personal data we hold about them. Requests can be made verbally or in writing to the Data Protection Lead.
- We may ask for proof of identity. We respond without undue delay and within **one month** of receiving the request (or, if later, of receiving any identification we need). For complex or multiple requests we may extend this by up to two further months, and will tell the requester within the first month and explain why.
- We ask for clarification only where it is reasonably required to respond effectively. In that case, the time limit pauses when we ask and resumes the day after the requester replies. We do not require a requester to narrow a valid request.
- We carry out reasonable and proportionate searches for the information requested. SARs are normally free of charge.

Correction and erasure

- If information we hold is inaccurate or out of date, we will correct it promptly.
- Individuals can ask us to delete their data. Where we have a legal obligation or another valid reason to keep certain records (for example, safeguarding, HMRC or insurance records), we will explain what we must retain and for how long. Deleting some information may mean we can no longer provide a service or continue a placement or employment.

14. Data protection complaints

Anyone who is unhappy with how we have handled their personal data can complain to us. Since 19 June 2026 organisations have been legally required to have a process for this.

- Complaints are accepted by any means, including by email to nicholas@proactiveyoungpeoplecic.co.uk, by post to Proactive Young People CIC, Proactive Office, Dunchurch Pools Marina, Onley, Rugby, Warwickshire CV23 8AN, or verbally to any member of staff, who will pass the complaint to the Data Protection Lead.
- We will **acknowledge the complaint within 30 days** of receiving it.
- We will investigate without undue delay, keep the complainant informed of progress, and tell them the outcome.
- We keep a record of data protection complaints and how they were resolved.

If someone remains dissatisfied, they can complain to the ICO: www.ico.org.uk, telephone 0303 123 1113. The ICO normally expects people to have raised their complaint with the organisation first.

15. Training, registration and review

- All staff, volunteers and placement students receive data protection training at induction and refresher training at least annually; training is recorded.
- ICO registration reference: ZA813873. The Data Protection Lead checks that the registration details and fee remain current.
- This policy is reviewed annually, or sooner if the law, guidance or our activities change.
- Related documents include our Safeguarding and Child Protection Policy, privacy notices, retention schedule, data protection records and relevant procedures and agreements. Staff should use the current versions of these documents and follow the school's instructions where PYP CIC processes information on its behalf.

This policy was adopted by: Proactive Young People CIC	Date: 29 September 2026
To be reviewed: September 2027	Signed: N. Brosnan, CEO / Data Protection Lead
Version: 2.1 (revised 29 September 2026; replaces version 2.0)	Reviewed against: UK GDPR and DPA 2018 as amended by the Data (Use and Access) Act 2025