Data Protection Policy

Your information. Your rights. Our responsibility.

This document explains what your rights are in protecting your data and how we make sure we respect them.

As a Pink Skills staff member, mentor or facilitator, any time you handle personal information about a participant, a colleague, or anyone else connected to the programme, you are responsible for handling it properly.

The short version

We only collect information we genuinely need. We keep it safe. We are honest about how we use it. We never sell it or share it carelessly. And we will always tell you what we hold about you if you ask.

What Is Personal Data?

Personal data is any information that can be used to identify a living person. That includes the obvious stuff like someone's name, email address or phone number. But it also includes less obvious things like a student identification number, an IP address, session notes that describe someone's circumstances, or a photograph.

There is also a category called special category data. This is personal data that is more sensitive because of what it reveals about a person. It includes:

- Health information and mental health records
- Information about disability
- Racial or ethnic origin
- Religious or philosophical beliefs

- Sexual orientation or sex life
- Biometric or genetic data
- Trade union membership
- Political opinions

Special category data gets extra protection because the potential for harm if it were misused is much greater. We treat it with the highest level of care.

In our programmes, special category data might include information shared during sessions about a participant's mental health, a disclosure about a disability, information about someone's ethnicity collected for equality monitoring, or a safeguarding record that describes someone's personal circumstances.

What Information We Hold and Why

We only collect and hold information that we actually need in order to run the programme properly, keep people safe, report our outcomes and fulfil our legal obligations. Here is what that looks like:

From participants

- Name, student number and contact details, so we can manage enrolment and get in touch about sessions
- Programme enrolment information and attendance records, so we can track participation and issue transcripts
- Session notes, which may include personal information shared in the course of mentoring or coaching
- Equality monitoring data such as ethnicity, disability status or age, collected anonymously to help us understand who is accessing the programme and whether outcomes are fair across different groups
- Safeguarding records where a concern has been raised, stored separately under strict access controls

From staff, mentors and facilitators

- Name, contact details and employment or engagement information
- DBS check details and training records
- References and recruitment documentation

From the university partner

- Referral information about students enrolled, shared under a data sharing agreement and only with student consent

The Seven Principles We Follow

UK GDPR sets out seven principles that every organisation handling personal data must follow. We have written them below in everyday language so they actually make sense.

1. Lawfulness, fairness and transparency

We process personal data on a proper legal basis. We are honest with people about what we do with their information. We do not do things behind people's backs.

2. Purpose limitation

We only use information for the reason we collected it. If we collect your email address to send you session reminders, we do not then use it to send you marketing messages. Simple.

3. Data minimisation

We only collect what we need. We do not collect personal information just because we might find it useful one day. If we do not need it, we do not ask for it.

4. Accuracy

We take reasonable steps to keep the information we hold accurate and up to date. If you tell us something has changed, we update it promptly.

5. Storage limitation

We do not keep personal information forever. We have a clear retention schedule (see the section on that later in this document) and we delete or anonymise data when it is no longer needed.

6. Integrity and confidentiality

We keep personal data secure. That means protecting it from being seen by people who should not see it, and from being accidentally lost, deleted or corrupted.

7. Accountability

We take responsibility for getting this right. We do not just say we comply with data protection law. We can demonstrate it.

Our Legal Basis for Processing Your Information

Every time we process personal data, we need a lawful basis for doing it. There are six possible bases under UK GDPR. Here are the ones we rely on and what they mean in practice:

Consent

You have given us clear, specific and informed permission to process your data for a stated purpose. You can withdraw consent at any time, and withdrawing it will not affect anything that happened before you withdrew it. We use consent as our basis for processing special category data such as equality monitoring information, and for sharing your information with the university partner.

Legitimate interests

We have a genuine and proportionate reason to process the data that does not override your rights and freedoms. For example, we have a legitimate interest in keeping records of session attendance for quality assurance purposes. Before we rely on this basis, we carry out a balancing test to make sure our interests do not outweigh yours.

Legal obligation

Sometimes the law requires us to process or share data. For example, if we receive a court order, or if a safeguarding situation means we must share information with a statutory authority. In these cases, we comply with the legal obligation even if we do not have your consent.

Vital interests

In an emergency where someone's life is at risk, we may process personal data to protect them, even without their consent. This is only used in genuine emergencies.

Your Rights

Under UK GDPR, you have real and enforceable rights over your personal data. Here is what they are in plain English:

The right to be informed

You have the right to know what personal data we hold about you, why we hold it, how long we keep it, and who we share it with. This policy is part of how we fulfil that right.

The right of access

You can ask us for a copy of all the personal data we hold about you. This is called a Subject Access Request, or SAR. It is free, and we have one calendar month to respond. To make a request, email info@pinkskills.org with your name and enough detail to help us find your information.

The right to rectification

If something we hold about you is wrong, you can ask us to correct it. We will do this promptly.

The right to erasure

Sometimes called the right to be forgotten. In certain circumstances, you can ask us to delete your personal data. This right does not apply in all situations, for example we cannot delete data we are legally required to keep, such as safeguarding records. But where it does apply, we will act on it.

The right to restrict processing

You can ask us to stop using your data in certain ways, for example if you dispute its accuracy or you have objected to our use of it and we are considering that objection.

The right to data portability

Where we process your data by automated means and on the basis of consent or contract, you can ask us to provide it in a structured, commonly used and machine-readable format so you can transfer it elsewhere.

The right to object

You can object to our processing your data where we rely on legitimate interests as our legal basis. When you object, we will stop processing unless we can demonstrate compelling legitimate grounds that override your rights.

Rights related to automated decision-making

You have the right not to be subject to a decision made purely by automated processing if that decision has a significant effect on you. Pink Skills does not currently use automated decision-making in this programme.

How to exercise your rights

Email: info@pinkskills.org with the subject line 'Data Rights Request'

We will respond within one calendar month of receiving your request.

There is no charge for exercising your rights.

How Long We Keep Your Information

We do not keep personal data longer than we need it. Here is our retention schedule:

What type of information	How long we keep it
Enrolment and contact details	3 years after you leave the programme
Attendance and session records	3 years after you leave the programme
Assessment and qualification records	7 years after your qualification is awarded
Safeguarding records	A minimum of 7 years (or longer if the matter is serious, ongoing or involves a child)
Equality monitoring data	Anonymised after 1 year and retained for statistical purposes for 7 years
Staff and mentor employment records	6 years after the end of your engagement with us
Financial and contractual records	6 years in line with HMRC requirements
Data breach records	5 years minimum

When data reaches the end of its retention period, we delete it securely. Digital data is permanently deleted from our systems. Physical documents are shredded.

How We Keep Your Information Safe

We take the security of personal data seriously. Here is what we do:

- All digital data is stored in password-protected systems with encryption enabled
- Access to personal data is restricted to the people who genuinely need it for their role
- Special category data, including safeguarding records and health information, is stored in separate, more tightly restricted systems

- We do not send personal data over unencrypted email. If we need to share sensitive information electronically, we use secure methods
- Physical documents containing personal data are stored in locked cabinets and shredded when no longer needed
- All staff complete data protection training before they access any personal data
- We carry out a Data Protection Impact Assessment before introducing any new process that involves high-risk data processing

We cannot guarantee that any system is completely secure, but we take every reasonable step to protect your information.

When We Share Your Information

We do not sell your personal data. We do not share it carelessly. But there are situations where we do share information, and we want to be upfront about them.

With statutory authorities in safeguarding situations

If a safeguarding concern requires us to share information with a local authority, the police, the NHS or another statutory body, we will do so regardless of whether we have your consent, because your safety or someone else's takes priority. In most cases, we will tell you that we are doing this. In situations where telling you would put you or someone else at greater risk, we may not.

With legal or regulatory bodies

If we receive a court order or are required by law to disclose information, we will comply.

In every other situation, your information stays with us. Data sharing agreements are in place with all third parties who receive personal data from Pink Skills, confirming that they will handle it in accordance with UK GDPR.

Confidentiality and Its Limits

Confidentiality is one of the foundations of our programme. The things people share in mentoring and coaching sessions are treated with real discretion. We do not gossip. We do not share unnecessarily. We treat personal information with respect.

But confidentiality is not absolute. There are specific circumstances where we have a duty to share information even without consent, and participants are informed about this clearly when they join the programme. Those circumstances are:

- When someone's life is at risk, including their own
- When a child or vulnerable adult is at serious risk of harm
- When a serious crime has been committed or is about to be
- When we are legally required to share information

In every other situation, we ask before we share. We explain what we need to share and why. And we document our decision in our records.

This is where data protection and safeguarding come together. When a safeguarding concern overrides confidentiality, it also overrides the usual data protection principle of needing consent to share. The law recognises this, and so do we. But we always act thoughtfully, not carelessly.

Special Category Data and Safeguarding Records

Safeguarding records contain some of the most sensitive personal data we hold. A record that describes why a student was referred to ARISE, or that documents a disclosure made during a session, is special category data in the deepest sense. It deserves extraordinary care.

We handle safeguarding records as follows:

- They are stored in a separate, encrypted system with access restricted to the Designated Safeguarding Lead, the Deputy DSL and senior leadership
- They are never included in general programme reports or shared with other participants
- They are only shared with the university or external agencies when there is a specific, documented safeguarding reason
- They are retained for a minimum of seven years, or longer if the matter is serious or ongoing
- They are written in factual terms, using the person's own words where possible, without assumptions or judgements

Equality monitoring data, such as information about ethnicity, disability or mental health, is treated as special category data. It is collected with explicit consent, stored securely, anonymised as quickly as possible, and used only for the purpose of understanding and improving the fairness and accessibility of the programme.

Data Breaches

A data breach is when personal data is accidentally or unlawfully lost, destroyed, altered, disclosed or accessed without authorisation. Data breaches do not just mean hacking. They include things like sending an email to the wrong person, losing a device that contains personal data, or accidentally giving someone access to a file they should not see.

If you think a data breach has happened, here is what to do:

1. Tell the Data Protection Lead immediately. Do not wait to see if it turns out to be nothing. Report it first.
2. Write down what happened, when, what data was involved and who might be affected.
3. The Data Protection Lead will assess the risk. If the breach is likely to put someone's rights or freedoms at risk, it must be reported to the Information Commissioner's Office within 72 hours of us becoming aware of it.
4. If the breach is likely to cause a high risk of harm to individuals, those individuals must be told directly and promptly.
5. All breaches are recorded in our data breach register, even if they do not need to be reported to the ICO.

Important: The 72-hour clock starts when Pink Skills becomes aware of the breach, not when it happened. If you know about it and you do not report it internally, that clock is already running.

Cookies and Digital Tools

Where Pink Skills uses a website, digital platforms or online tools as part of its programme delivery, it will comply with the Privacy and Electronic Communications Regulations (PECR) in addition to UK GDPR. This means:

- We will be transparent about any cookies or tracking tools used on our digital platforms
- We will obtain consent before placing non-essential cookies on a user's device
- We will only use approved, secure platforms for online sessions
- We will not record online sessions without the explicit consent of all participants

Where This Policy Connects to Others

Data protection does not sit on its own. It runs through the rest of our work in important ways.

- Safeguarding Policy: When safeguarding requires us to share personal information without consent, this is lawful under UK GDPR on the basis of vital interests or legal obligation. The two policies work together. Safeguarding always comes first, but we still handle data thoughtfully even in an emergency.
- Equality, Diversity and Inclusion Policy: Equality monitoring data is special category data. It is handled with explicit consent and subject to the full protections in this policy. You are never required to provide equality monitoring data as a condition of joining the programme.
- Confidentiality: The limits of confidentiality described in this policy are the same limits described in our Confidentiality Policy. They are consistent and intentional.
- Safer Recruitment: DBS records and recruitment data are personal data and are handled in full compliance with this policy.
- Whistleblowing: If you believe Pink Skills is mishandling personal data, you can raise this without fear of retaliation through the Whistleblowing Policy, or directly with the ICO.

Complaints About How We Handle Your Data

If you are not happy with how we have handled your personal data, please tell us. You can raise a concern at any time by emailing info@pinkskills.org We will respond within 20 working days.

Reviewing and Updating This Policy

This policy is reviewed every year by the Data Protection Lead and senior leadership. It is also updated sooner if there are changes in legislation or guidance, or if an incident reveals something we need to do differently.

The UK data protection landscape is changing. The Data (Use and Access) Act 2025 introduced reforms to how personal data can be processed and shared in certain contexts. We monitor developments closely and update our practices accordingly.

This policy is version 1.0, effective from April 2026.

Next review: April 2027.

Questions? info@pinkskills.org