

Confidentiality & Data Protection Policy

POLICY APPROVAL					
Approval Required	Indicate with a tick (✓)		**Annual Review Required**	Indicate with a tick (✓)	
	Yes ✓	No		Yes ✓	No
Approval Panel	Loren Janes				
Approved by	Name: Loren Janes		Signature: 	Date: September 2025	
Policy Review Date	September 2026				

Policy Statement

During the course of our activities, we will process personal data (which may he held on paper, electronically, or otherwise) about our staff and we recognise the need to treat it in an appropriate and lawful manner, in accordance with the Data Protection Act 2018 (DPA). The Data Protection Act 2018 is the UK implementation of the General Data Protection Regulations (GDPR). The purpose of this policy is to make you aware of how we will handle your personal data. The policy does not form part of any employee's contract of employment, and we may amend it at any time.

We are registered with the ICO (Information Commissioners Office), the UK's independent authority set up to uphold information rights in the public interest.

Scope

All employees, learners', and other stakeholders' data is stored, shared and utilised as described within this policy.

Data protection principles

Everyone responsible for using personal data has to follow strict rules called 'data protection principles. They must make sure the information is:

- Used fairly, lawfully and transparently
- Used for specified, explicit purposes
- Used in a way that will adequate, relevant and limited to only what is necessary
- Accurate and, where necessary, kept up to date
- Kept for no longer than necessary
- Handled in a way that ensures appropriate security, including protection against unlawful or unauthorised processing, access, loss, destruction or damage

"Personal data" means recorded information we hold about you from which you can be identified. It may include contact details, other personal information, photographs, expressions of opinion about you or indications as to our intentions about you. "Processing" means doing anything with the data, such as accessing, disclosing, destroying or using the data in any way

Fair and lawful processing

We will usually only process your personal data where you have given your consent or where the processing is necessary to comply with our legal obligations. In other cases, processing may be necessary for the protection of your vital interests, for our legitimate interests or the legitimate interests of others. The full list of conditions is set out in the DPA.
We will only process "sensitive personal data" about ethnic origin, political opinions, religious or similar beliefs, trade union membership, health, sex life, criminal proceedings or convictions, where a further condition is also met. Usually this will mean that you have given your explicit consent, or that the processing is legally required for employment purposes. The full list of conditions is set out in the DPA.

How we are likely to use your personal data

We will process data about staff for legal, personnel, administrative and management purposes and to enable us to meet our legal obligations as an employer, for example to pay you, monitor your performance and to confer benefits in connection with your employment.
We may process sensitive personal data relating to staff including, as appropriate:

a) Information about an employee's physical or mental health or condition in order to monitor sick leave

and take decisions as to the employee's fitness for work

b) The employee's racial or ethnic origin or religious or similar information in order to monitor compliance with equal opportunities legislation
c) In order to comply with legal requirements and obligations to third parties

Processing for limited purposes

We will only process your personal data for the specific purpose or purposes notified to you or for any other purposes specifically permitted by the DPA.

Safeguarding and KCSIE 2025

The organisation recognises that information collected and processed as part of our safeguarding responsibilities constitutes personal data and, in many cases, special category data. This includes records relating to safeguarding concerns, child protection, welfare issues, allegations, and referrals.

In line with the Keeping Children Safe in Education (KCSIE) 2025 statutory guidance, safeguarding takes precedence over data protection where there is a risk of harm to a child or vulnerable person. The General Data Protection Regulation (GDPR) and the Data Protection Act 2018 are not a barrier to sharing information but provide a framework to ensure that personal information about children, young people, and families is shared appropriately.

Safeguarding information will only be shared with those who need to know, in order to protect the welfare of the learner. This may include internal safeguarding leads, local safeguarding partners, law enforcement, health professionals, or social care services. Staff are required to follow the organisation's safeguarding procedures and escalate concerns without delay.

Records relating to safeguarding will be:

- Stored securely and separately from general learner files.
- Restricted to authorised safeguarding staff only.
- Retained in line with statutory guidance, normally until the learner reaches their 25th birthday, unless legal or regulatory requirements specify otherwise.

All staff receive regular training on confidentiality and information sharing in the context of safeguarding and are reminded that the safety of the child is paramount when making decisions about sharing information.

The organisation uses CPOMS to securely record and manage safeguarding, welfare, and child protection concerns. CPOMS is a cloud-based system that ensures safeguarding information is stored in accordance with the Data Protection Act 2018 and the UK GDPR. Access to CPOMS is strictly limited to authorised staff, including the Designated Safeguarding Lead (DSL) and deputies, and is role-based to ensure confidentiality.

All entries are time-stamped and logged, creating an audit trail of safeguarding activity. Records are encrypted and held on secure servers located in the UK, with appropriate technical and organisational measures in place to prevent unauthorised access, alteration, or loss.

CPOMS supports lawful information sharing as required under KCSIE 2025**,** ensuring that safeguarding records are transferred securely when a learner moves to another provider. These transfers are completed electronically via CPOMS, reducing the risk of data breaches associated with paper files.

Staff receive training in how to use CPOMS in line with safeguarding and data protection responsibilities. The safety of the learner remains the overriding priority in all decisions regarding information management.

Data Sharing and Transfers

Futures Changing Ltd will only share personal data where it is lawful, proportionate, and necessary to fulfil its educational, safeguarding, and legal obligations. Data may be shared with:

- **Government bodies and regulators** such as the Department for Education (DfE), the Education and Skills Funding Agency (ESFA), Ofsted, and local authorities.
- **Awarding bodies and examination boards** for the purpose of certification and assessment.
- **Safeguarding partners**, including local safeguarding boards, social care, law enforcement agencies, and healthcare professionals, where necessary to protect children or vulnerable adults.
- **Service providers and contractors** who process data on our behalf, subject to strict contractual safeguards to ensure compliance with data protection legislation.

Futures Changing Ltd does not transfer personal data outside the UK unless adequate safeguards are in place. Where international transfers are necessary, they will only occur if:

- The country has been deemed to provide an adequate level of data protection by the UK government; or
- Appropriate safeguards, such as standard contractual clauses, are in place; or
- The data subject has given explicit consent.

All data sharing is logged and monitored to ensure accountability, and data subjects are informed of how their data may be shared through our Privacy Policy.

CCTV Recording

We have a CCTV surveillance system in place at Futures Changing This includes both images and audio of staff, learners and visitors to the centre. As an Internet Testing Centre, we are required to ensure tests are controlled. Cameras are sited to ensure they cover test stations and can be used to validate tests, user integrity and security. Additional cameras are at the front and the rear of the property for security reasons. The CCTV system is operational and is capable of monitoring 24 hours a day, every day of the year. Images are stored on a server located securely in the building. CCTV images and audio recordings will be retained for no longer than 30 days from the date of recording unless these are requested by CITB as part of an ongoing investigation. Images will be automatically overwritten after this point. All images recorded by the CCTV System remain the property and copyright of Futures Changing. We may supply the CITB with footage of learners at a particular time in order to validate or identify a particular test or learner.

Adequate, relevant and non-excessive processing

Your personal data will only be processed to the extent that it is necessary for specific purposes as you are notified.

Accurate data

We will keep the personal data we store about you accurate and up to date. Data that is inaccurate or out of date will be destroyed. Please notify us if your personal details change or if you become aware of any inaccuracies in the personal data, we hold about you.

Data retention

We will not keep your personal data for longer than is necessary for the purpose. This means that data will be destroyed or erased from our systems when it is no longer required.

Processing in line with your rights

You have the right to:

(a) Request access to any personal data we hold about you

(b) Prevent the processing of your data for direct marketing purposes

(c) Ask to have inaccurate data held about you amended

(d) Prevent processing that is likely to cause unwarranted substantial damage or distress to you or anyone else

(e) Object to any decision that significantly affects you being taken solely by a computer or other automated process

Data security

We will ensure that appropriate measures are taken against unlawful or unauthorised processing of personal data, and against the accidental loss of, or damage to, personal data. We have in place procedures and technologies to maintain the security of all personal data from the point of collection to the point of destruction. We will only transfer personal data to a third party if he agrees to comply with those procedures and policies, or if he puts in place adequate measures himself. Maintaining data security means guaranteeing the confidentiality, integrity and availability (for authorised purposes) of the personal data.

Providing information to third parties

We will not disclose your personal data to a third party without your consent unless we are satisfied that they are legally entitled to the data. Where we do disclose your personal data to a third party, we will have regard to the eight data protection principles.

Subject access requests

If you wish to know what personal data we hold about you, you must make the request in writing, with an accompanying fee of £10. All such written requests should be forwarded to the manager.

Breaches of this policy

If you consider that this policy has not been followed in respect of personal data about yourself or others you should raise the matter with your line manager. Any breach of this policy will be taken seriously and may result in disciplinary action.