



Confidentiality Policy

Kate's Training CIC

1. Purpose

This policy explains how Kate's Training CIC ("the CIC") protects confidential information and when that information may be used or shared. It helps us work lawfully, fairly and securely, protect the rights and dignity of learners and others, and maintain trust in our services. Read it alongside the CIC's Data Protection and Privacy, Safeguarding, Information Security, Records Retention, Whistleblowing, Complaints and Disciplinary policies.

2. Scope

This policy applies to all directors, employees, sessional workers, tutors, assessors, volunteers, contractors, consultants, placement staff and anyone working on behalf of the CIC. It covers confidential information in any form, including conversations, paper records, photographs, recordings, emails and electronic files. It applies whether the information is used on site, remotely or while travelling.

3. Definition of Confidential Information

Confidential information is information that is not publicly available and would reasonably be expected to remain private and protected. This includes:

- personal information about learners, prospective learners, staff, volunteers, contractors, clients, partners, donors and other contacts;
- sensitive personal information, such as health, disability, ethnicity, religion or belief;
- safeguarding concerns, disclosures, referrals and case records;
- assessment evidence and records of reasonable adjustments, attendance, progress, support needs and results;
- financial information, including funding records, fees, payroll and bank details;
- commercial, contractual, operational, technical or strategic information;
- passwords, access details, security arrangements and incident records; and
- information given to the CIC in confidence by another person or organisation.

4. Core Principles

Kate's Training CIC will:

- use confidential information only for lawful and authorised purposes;
- give access only to people who need the information for their work;
- collect and keep only the information that is needed;
- keep information accurate, secure and only for as long as required;
- share only the minimum information needed and use secure methods;
- explain how information will be used, where appropriate; and
- record important decisions about sharing information and the reasons for them.

5. Responsibilities

5.1 Board of Directors

The Board is responsible for making sure effective confidentiality arrangements are in place. It will keep this policy up to date, provide guidance, oversee training and incidents, and ensure that suitable controls, contracts and records are maintained.

Kate's Training CIC is a community interest company limited by guarantee registered in England and Wales (Registration number 15816406).



5.2 Responsibilities of All Personnel

- understand and follow this policy and any procedures that apply to their role;
- access, discuss, copy, photograph, remove or share confidential information only when they have a genuine work-related need and permission;
- check the identity and authority of anyone receiving confidential information;
- immediately report mistakes, suspected breaches, lost information, unauthorised access or inappropriate disclosure;
- return or securely dispose of confidential information when instructed or when their role ends; and
- continue to protect confidential information after their work with the CIC ends.

6. Secure Handling

- Store paper records securely and do not leave them visible or unattended.
- Keep electronic records in approved systems. Protect them with strong passwords and, where available, multi-factor authentication.
- Do not send confidential information to personal email accounts, store it on unapproved devices or services, or discuss it using unapproved messaging applications.
- Check recipients and attachments before sending. Where appropriate, protect sensitive files or share them through an approved secure link.
- Lock screens when they are unattended and hold confidential conversations where others cannot overhear them.
- When working remotely, protect privacy at home and in public places, use approved systems, and prevent access by household members or anyone else who is not authorised.
- Shred confidential waste or use an approved secure disposal service.

7. Sharing and Disclosure

Confidential information may be shared only when there is a lawful and legitimate reason, the recipient is authorised, and the amount shared is appropriate. This may include sharing:

- with colleagues who need it to provide training, assessment, learner support, administration or governance;
- with funders, awarding organisations, regulators, professional advisers, insurers or contracted service providers when necessary and properly protected;
- with the person's valid consent, when consent is the appropriate basis;
- to meet a legal duty, court order or regulatory requirement;
- to prevent or detect crime, fraud or serious wrongdoing, where lawful;
- to protect someone's life or safety, or respond to a serious and immediate risk; or
- for safeguarding purposes, when sharing is needed to protect a child or adult at risk.

Confidentiality has limits. Nothing in this policy prevents employees or workers from reporting a crime, raising a safeguarding concern, making a protected disclosure under whistleblowing law, seeking confidential legal or healthcare advice, using their legal rights, or assisting an authorised investigation.

If you are unsure whether information should be shared, ask the policy owner or designated safeguarding lead before sharing it. The only exception is when waiting would create an immediate risk of harm.

8. Safeguarding Information

Safeguarding information is highly sensitive and must be shared only with people who need to know. Staff and volunteers must never promise to keep a safeguarding disclosure completely secret. They should listen, avoid unnecessary questions, make an accurate and factual record, and report the concern promptly under the



Safeguarding Policy. Information may be shared without consent when this is lawful and necessary to protect a child or adult at risk.

9. Meetings, Teaching and Communications

- Do not discuss confidential learner or staff matters in open areas or with people who do not need the information.
- Remove identifying details from case examples used in teaching, unless there is a clear lawful reason and appropriate authority to name the person.
- Use approved platforms and suitable privacy settings for online sessions. Record a session only when this is authorised, necessary and clearly explained.
- Remind group participants to respect each other's privacy. Make clear that the CIC cannot guarantee that other participants will keep information confidential.

10. Confidentiality Incidents and Breaches

Immediately report any actual or suspected loss, unauthorised access, accidental disclosure, misdirected message, insecure disposal or other confidentiality breach to the policy owner using the CIC's incident-reporting process. Preserve any evidence, follow instructions to contain the issue, and do not hide the incident.

The CIC will act promptly to contain and assess the incident. It will record decisions, consider the risk to affected people, notify individuals or authorities when required, and take steps to prevent the issue from happening again. Personal data breaches will also be managed under the Data Protection and Privacy Policy and any legal reporting duties.

11. Training, Monitoring and Compliance

The CIC will provide induction and refresher training based on each person's role and the level of risk. It may monitor compliance through supervision, access controls, audits, incident reviews and contract management. Intentional or careless breaches may lead to restricted access, disciplinary action, termination of employment or engagement, recovery of losses, or referral to regulators or law-enforcement authorities, as appropriate.

12. Review and Contact

This policy will be reviewed at least once a year. It will also be reviewed sooner after a major incident, a change in law or regulation, or a significant change to the CIC's work. For questions, concerns or guidance, contact: kate@katestraining.uk or support@katestraining.uk.

Policy owned and approved by	Board of Directors at Kate's Training CIC
Policy team	K. Gorski, K. Metcalfe, D. Gorski, E. Adelakun
Main contact	Kate Gorski, kate@katestraining.uk , 01617062276, 07362512257
Effective date	1 st September 2026
Next review	1 st September 2027, or as and when required
Applies to	Directors, Employees, Workers, Volunteers, Trainers, Contractors