

Safeguarding Adults at risk

Policy and procedures

Version 1.0

Approved by Sharon Sanders Founder/CEO

Date: 1st June 2026 Review annually and after any statutory changes

Purpose and scope

Digital You CIC delivers digital inclusion activities on host organisations' premises, with their staff, members, and clients. This policy applies to everyone representing Digital You, including directors, employees, associates, and volunteers. We will prevent harm where possible, listen to concerns and act promptly. Our role is to recognise, respond, record and report; statutory agencies investigate suspected abuse.

An adult is someone aged eighteen or over. The Care Act safeguarding threshold concerns someone with care and support needs who is experiencing or at risk of abuse or neglect and, because of those needs, cannot protect themselves. This applies whether or not the council meets those needs. Digital exclusion, disability, age, or limited English alone do not establish that threshold. Seek advice about any safety concern even where the threshold is unclear.

Digital You responsibilities

Sharon Sanders, Founder/CEO, is the Designated Safeguarding Lead (DSL). She oversees safeguarding, supports the team, coordinates reporting and follow-up, and keeps secure records. A deputy, Ayisha Hameed provides cover and acts where Sharon is unavailable or implicated. Directors approve the policy and ensure appropriate recruitment, training, and cover during delivery. Everyone must act on concerns without waiting for permission when someone is at risk.

Working with the host organisation

Before the first session, the person coordinating the booking confirms a short-written safeguarding arrangement with the host. It names both organisations' contacts, local referral routes, how concerns will be shared and who will refer and follow up. The coordinator passes this to the delivery lead. Before each session, the delivery lead checks the team has these details, knows who is available and understands how to report concerns, and explains the reporting route to participants.

The host will normally coordinate support and referrals concerning its own members or clients, as agreed for the activity. Digital You remains responsible for its people's conduct, safe delivery, reporting concerns and checking that action happens. The booking coordinator or delivery refers to gaps or concerns to the DSL or deputy, who agrees to a safe alternative before delivery proceeds. Routine booking checks do not require DSL's personal involvement or sign-off.

Agree any participant support needs, accessibility adjustments and who will provide support during sessions. Digital You workers must stay within their agreed role and must not take on personal care, control of finances or other responsibilities by default.

Recognising concerns and working safely

Abuse may be physical, sexual, psychological, financial, or discriminatory. It also includes domestic abuse, neglect, organisational abuse, modern slavery, and self-neglect. It may be a single event or a pattern, online or offline, involving a worker, relative, another participant or a stranger.

Possible signs include unexplained injury, fear or withdrawal, unmet basic needs, missing money, scams, pressure to share passwords, or someone controlling the adult's device and answering for them. These signs are not proof. Note what you observe, listen, and seek advice. Consider risks to others, including children, and exploitation such as forced marriage or grooming into terrorism.

The Adult's wishes and capacity

Ask what the adult wants to happen. Apply empowerment, prevention, proportionality, protection, partnership, and accountability. Presume capacity, explain options accessibly and support decisions. An unwise choice does not itself show incapacity. Capacity is specific to the decision and time; seek specialist advice if it is in doubt. Where capacity is lacking, follow the Mental Capacity Act, including best interests and the least restrictive option. Ask the council about independent advocacy where needed.

People and session arrangements

Check identity, relevant experience, references, and suitability before appointing workers. Assess DBS eligibility for each role; request enhanced or barred list checks only where legally eligible. Do not assume every digital inclusion role qualifies. Record checks, supervision and any relevant restrictions, respecting conviction filtering rules.

Everyone must understand these policies and complete training appropriate to their role before unsupervised delivery. Sharon and the deputy need training for safeguarding decisions and local referral procedures. Provide an annual update and further briefing when risks or guidance change. Agree staffing and any one-to-one support with the host; keep support visible and avoid isolated contact. Use appropriate communication support and independent interpretation where needed.

Safe digital support and conduct

- Explain each task and obtain permission before viewing information or touching a device. Use demonstration accounts where possible. Never retain passwords, PINs, or security codes, move money, or become a participant's account recovery contact.
- Keep participants in control. If a sensitive task needs more support, arrange suitable authorised help. Sign out of shared devices, remove temporary personal files securely and protect screens from others.
- Use approved work contact channels. No private social media contact, exploitative relationships, inappropriate gifts, or unplanned private visits. Declare existing relationships and manage any conflict.
- Protect privacy. Do not take or publish images without appropriate permission or upload identifiable learners or safeguarding information to public AI tools. Report boundary breaches and unsafe practice.

What to do if you have concerns

1 Make the person safe.

Call 999 for immediate danger or urgent medical help. Give the location and known facts. Take safe protective action and alert the host's person responsible where appropriate. Do not wait for a manager or put yourself or others at risk.

2 Listen and explain.

Stay calm, take the concern seriously and reassure the person that they were right to tell you. Explain that you may need to share information to help keep people safe. Do not promise secrecy, ask leading questions, investigate or confront the alleged abuser. Ask only what is needed for safety and reporting.

3 Report promptly.

Tell Sharon or the deputy immediately and always on the same day. Share with the host's safeguarding lead where necessary and safe, following the agreed arrangement and the consent principles below. Do not share with someone implicated in the concern. If a lead is unavailable or delay creates risk, contact statutory services directly.

Seek the adult's agreement to sharing and referral wherever possible. If an adult with capacity declines, consider their wishes and any coercion. Sharing without consent requires lawful, proportionate justification, such as serious risk to others, a legal requirement, or an overriding public interest. A suspected crime does not automatically override every adult's wishes. Seek safeguarding advice and record the reasons for the decision; do not delay emergency action.

4 Record and confirm action.

Write down what happened as soon as safe, normally the same day. Use the form in this policy or the host's form if it captures the same information. Record exact words where possible, observations, decisions, the person's wishes, and action taken. Keep a secure Digital You record of the concern and its response; do not delay a referral to finish a form.

Agree who is making any referral and by when. Sharon or the deputy must obtain confirmation that it was received and record the next steps. Telling the host alone does not close the concern. If a referral is not needed, record why, any support offered and when the situation will be reviewed.

5 Follow up or escalate.

Follow up with adult safeguarding within the response time agreed when referring; act sooner if risk increases. If the host does not act, is implicated, or neither organisation remains concerned, refer directly and use the local safeguarding escalation procedure. Anyone can contact statutory services without internal permission. Keep the person informed where safe to do so.

Digital evidence

Do not search devices or copy potentially illegal images. Record available non-image details and seek police or social care advice about preserving evidence. Do not delete potential evidence or circulate it in a report. Consider whether changing settings or blocking a person could increase danger.

Allegations information and oversight

Concerns about a worker

Report immediately any allegation or behaviour suggesting that a Digital You or host worker may have harmed someone or be unsuitable for their role. Include relevant behaviour outside work and smaller boundary concerns that may form a pattern. Use an unimplicated lead. Concerns about Sharon go to the deputy or directly to the relevant statutory service; concerns involving both leads directly to statutory services.

The unimplicated DSL or director must promptly consult local adult safeguarding and follow its procedure for allegations about people in positions of trust. Contact police where required and consider any risk to children. Agree who is notifying statutory services for a host worker and confirm this has happened.

Do not investigate or alert the person accused in a way that could compromise protection or evidence. Agree next steps with statutory services. Record proportionate interim measures, such as supervision or pausing delivery, and provide separate support to those involved. Directors must check and meet any applicable DBS referral duty, including qualifying cases where someone resigns, and relevant contractual or professional notifications. No one should face retaliation for raising an honest concern.

Information sharing and records.

Share only relevant and necessary information with appropriate people, using a secure method and checking recipients. Record what was shared, why and with whom, including the lawful basis and any additional condition for sensitive data. Explain sharing unless this increases risk or prejudice an investigation. Data protection must not prevent necessary lawful safeguarding action.

Keep safeguarding records in a restricted Digital You folder, separate from the general CRM and attendance lists. Limit access to those managing the concern, use multi-factor authentication and transfer paper notes securely. Do not keep case details in personal email or messaging apps. Agree a secure information exchange with the host without routinely copying its full client file.

Directors must approve retention periods for safeguarding concerns, allegations, and DBS information in the data retention schedule, taking account of applicable law, local safeguarding advice, and insurer requirements. Record review dates, delete securely when justified and suspend deletion for investigations or claims.

Review and learning.

Directors review this policy annually and sooner after a serious incident, relevant guidance change or change in delivery. Check training, reporting and follow-up, and record improvements. Any work outside the host-premises model, including home visits or standalone online delivery, needs its safeguarding arrangements reviewed before it begins.

Contacts and supporting guidance.

The DSL or deputy confirms internal contacts and covers before adoption. The booking coordinator maintains a short contact sheet for each host and shares it with the delivery team. An existing host sheet may be used. For repeat sessions, reuse the agreed arrangements; the delivery checks for changes before delivery and reports any updates or gaps.

Digital You contacts.

Designated Safeguarding Lead: Sharon Sanders, Founder/CEO

Work telephone and secure email: sharon@digitalyou.org.uk 0191 7169565

Deputy Safeguarding Lead: ayisha@digitalyou.org.uk 0191 7169565

Concerns involving both internal leads must go directly to the relevant statutory service. A concern about a lead must not be referred back to that person for a decision. Emergency police or ambulance 999; non-emergency police 101.

Agree once with each host.

The booking coordinator records the host organisation and venue, its safeguarding lead and cover contact, and how to reach them during sessions. Include the relevant local authority referral team, out-of-hours emergency duty contact and position of trust allegations route.

- Who provides participant support and supervision, including childcare where relevant.
- How Digital You and the host will share concerns safely and who will refer to statutory services.
- How receipt, follow-up and escalation will be confirmed, with a named owner.
- How participants can raise concerns verbally or in writing, with suitable communication support.

Use the local authority covering the concern or delivery location and involve the person's home authority where relevant. Ask the receiving service to resolve cross-boundary arrangements; do not delay protection over responsibility disputes. Digital You's secure record location and retention schedule must be agreed before adoption.

Safeguarding concern record

Confidential safeguarding record. Complete promptly and send securely to the DSL or alternative contact. Record only what is known; do not investigate or delay urgent action to fill gaps. Use continuation sheets as needed.

Report details

Date and time of report; your name, role, and safe contact details; session or location.

Person concerned

Name; age or date of birth if known; current location; safe contact method; communication and accessibility needs.

Concern and source

Date and time of incident or disclosure; what you saw or heard; exact words where possible; who else was present. Distinguish facts, third-party information, and opinion.

Immediate safety

Current risks; others at risk; emergency action; medical help, whether the alleged person still has access.

Views and information sharing

Adult's wishes and desired outcome; consent sought or given; decision-specific capacity concerns; reasons for any sharing without consent.

Reporting and referrals

DSL or alternative notification; agency, named recipient, date, and time; reference number; information shared and secure method.

Decisions and follow-up.

Advice received; decision and reasons, including any decision not to refer; action owner and deadline; referral receipt and outcome; escalation if needed.

Completion

Reporter and date; DSL review and date; next review; secure record reference; retention review date.