

E-Safety Policy

Positive Smiles C.I.C.

Document control

Published Date:	03/12/2018	Author:	Shabir Siddiq – Director
------------------------	------------	----------------	--------------------------

Version	Change Detail	Latest Review Date	Date of Next Review	Updated By:
1.0	Annual Review	03/12/2019	03/12/2020	Shabir Siddiq
1.0	Annual Review	03/12/2020	03/12/2021	Shabir Siddiq
1.0	Annual Review	07/12/2021	07/12/2022	Shabir Siddiq
1.1	Annual Review & Policy Amended	07/12/2022	07/12/2023	Shabir Siddiq
1.1	Annual Review Changed to Academic Year Start	01/08/2023	31/07/2024	Shabir Siddiq
1.2	Annual Review	01/08/2024	31/07/2025	Shabir Siddiq
1.3	Annual Review & header logo change	01/08/2025	31/07/2026	Shabir Siddiq
1.4	Annual review, Positive Smiles rebrand and realignment to adult services	01/08/2026	31/07/2027	Shabir Siddiq

INTRODUCTION

This policy sits alongside Positive Smiles' Acceptable Use Policy, AI Usage Policy, Data Protection & Confidentiality Policy and Staff Code of Conduct. All staff and volunteers should make sure they know what these policies require.

The internet and digital tools bring real benefits for the adults we support, from job searching and online learning to keeping in touch with family. They also bring risks. Adults can be targeted by scams, fraud, online grooming and exploitation. Some participants, including those new to the UK, those still learning English and those with low digital confidence, may find these risks harder to spot.

E-safety is about keeping participants, staff and volunteers safe from risks to their personal safety, wellbeing and money when using devices that access the internet or communicate electronically. This includes computers, mobile phones, tablets, social media, messaging apps and AI tools.

To help participants stay safe online, staff and volunteers need a working awareness of the sites, apps and tools participants use and the risks linked with them.

All staff and volunteers are expected to complete the e-safety training provided by Positive Smiles.

This policy aims to provide staff and volunteers with:

- An awareness of the risks faced by adults using digital technology, including AI tools.
- Guidance for dealing with e-safety issues, particularly for participants who may be at risk of harm or exploitation.
- An appreciation of professional boundaries and electronic technology.
- A reminder of Positive Smiles' expectations on internet use and the Code of Conduct.

ONLINE RISKS FOR ADULTS

Internet use in our sessions (including computers, laptops and mobile devices)

Positive Smiles devices and Wi-Fi used by participants should have suitable filters and security settings. Staff should explain the reasons for this to participants.

Scams and fraud

Participants may be targeted by phishing emails, fake texts, bogus job adverts, fake official messages and requests for money or bank details. Staff should help participants recognise the warning signs and check before they click, reply or pay.

Mobile phones

Most participants use a mobile phone as their main way to get online, often without filters or security settings. Phones can also be used to record and share images and messages. Once sent, these are beyond the owner's control.

Unwanted contact

Some participants may be at risk from people who are not allowed to contact them, or whose contact should be limited, for example in cases of domestic abuse. These people may use social media or messaging apps to make contact or to find out where a participant is.

Grooming and exploitation

People who wish to exploit adults may build a relationship online over weeks or months, for example through romance scams, false offers of work or housing, or radicalisation. Adults who are isolated or in vulnerable circumstances may be at greater risk.

Messaging and photo/video sharing

Messaging apps allow private conversations between people who have each other's contact details, and these are not moderated. There is a risk that participants may share images or personal information they later regret. Once shared, they have no further control over them.

Photo and video sharing apps allow images to be saved, screenshotted and passed on by the recipient in ways the sender did not intend.

Online groups and forums

Online groups and forums connect people with shared interests. Some are moderated, but many are not.

There is a risk that participants may form "friendships" with people who are not who they say they are, or be exposed to abusive or extremist content.

Social networking

Social media sites allow users to build networks, share opinions, photos and videos, and keep in touch. Many of the risks of online groups also apply, including fake profiles, abusive language and cyber bullying (see below). Most sites have a button to report posts or users that make someone feel uncomfortable.

Digital and AI confidence

Many of the adults we support are building their digital skills, and some use AI tools such as chatbots for job applications, translation and everyday tasks. Staff should help participants use these tools safely: not entering personal, financial or sensitive information; checking AI answers against trusted sources; and being aware that images,

voices and videos can be faked using AI. Any use of AI in our sessions must follow our AI Usage Policy.

Cyber bullying

Cyber bullying is bullying using information technology. It can include sending threatening or abusive emails or texts, making insulting comments, or making and sharing hurtful or embarrassing videos. Once information has been shared it is out of the originator's control and the abuse can spread, causing more distress to the victim.

Supporting victims and managing incidents

Where a participant is receiving unwanted or unsafe contact, staff should give them practical support to block and report the contact, and follow our safeguarding procedures where there is a risk of harm.

Where a participant has been the victim of bullying, abuse, fraud or inappropriate behaviour online, staff should identify suitable support in line with our Safeguarding Policy and record the concern. The participant should be advised not to respond to the abusive contact. Evidence (messages, emails, screenshots) should be saved and the Police contacted as appropriate. The Police should always be contacted about illegal activity, grooming or exploitation. Staff can help participants ask online providers to remove posts or images.

If a participant has used Positive Smiles equipment or Wi-Fi inappropriately, staff should discuss this with them and explain the risks. Activity that might be illegal should be reported to a Director.

The following advice may be helpful when supporting participants to stay safe online:

- Use strong, different passwords and turn on two-step verification where you can.
- Talk to a member of staff or someone you trust if you see anything that makes you feel uncomfortable.
- Close any webpage or message that makes you feel uncomfortable and report it.
- Do not give out personal information such as your address, date of birth or bank details.
- Never share passwords or one-time passcodes, or let anyone you do not know access your device.
- Ensure you set the correct privacy settings on social networking websites so that not everyone can see your details, pages and photos.
- Be careful about contact from people you have not met offline.
- Only accept friend requests from people you have actually met offline.
- Take care before meeting anyone you have only met online: meet in a public place and tell someone where you are going.
- Cover or switch off webcams when not in use.

- Think very carefully about any pictures and comments you post online as these may be forwarded on without your knowledge or permission and become out of your control.
- Never be abusive or unkind to anyone on the internet.
- Only open emails and links from people and organisations you recognise.
- Be wary of anyone asking for money, gift cards or bank transfers.
- Check information from websites and AI tools against trusted sources, such as GOV.UK.

EMPLOYEE ISSUES & PROFESSIONAL BOUNDARIES

Internet usage (including computers, laptops and mobile devices)

Whilst at work, employees must not visit internet sites, make, post, download, upload or pass on material remarks, proposals or comments that contain or relate to:

- Indecent or illegal images.
- Promoting discrimination of any kind.
- Promoting racial or religious hatred.
- Promoting illegal acts.
- Violence and bomb making.
- Illegal taking or promotion of drugs.
- Adult pornography.
- Other information that may be offensive to others.

Illegal activity will be reported to the Police.

Employees need to be aware of professional boundaries and expectations in relation to the internet and electronic technology. Employees should not take photos or videos of participants using their personal

equipment. Employees should use a work-owned and approved device for permitted photography, and only with the person's consent. Photos and videos must be stored appropriately and, once uploaded or printed as required, deleted from the original device. Any images temporarily taken home (e.g. after an event when equipment cannot be returned to the office until the next working day) must be stored securely and in line with data security expectations.

Employees must consider and review the way they use social networking. Security settings should be used to control access to profiles. Employees need to be aware that once published, information including photographs and posts, may be manipulated without consent, used in a different context or distributed in an uncontrolled way.

It is not appropriate for employees to have participants as friends on their personal social media. Employees should avoid detailed discussion about work on social media to avoid any unintentional lapse in confidentiality. Employees should not upload any work-related images or “tag” their location. Employees should only use work-provided equipment and accounts to make electronic contact with participants, and should note all electronic contact with participants in their records.

If in doubt employees should contact their line manager for advice and/or refer to the Staff Code of Conduct.

REPORTING ABUSE AND MISUSE

It is the responsibility of all employees to report any abuse and misuse of the internet by colleagues to their line manager in the first instance. Employees should refer to Positive Smiles’ Whistleblowing Policy.

Employees should also inform the Designated Safeguarding Lead (DSL) within 1 working day and follow company procedures.

Where there has been inappropriate or illegal use of the internet by an employee:

- Employees may be subject to Positive Smiles’ disciplinary process. Accessing certain sites may be considered gross misconduct and may lead to dismissal without notice.
- Serious breaches and illegal activity will be reported to the Police. A Director and/or the DSL must be contacted before this is progressed. A decision will be made as to whether the incident needs an internal investigation.

If concerns are raised about an employee or representative of another agency, these should be reported immediately to a Director and/or the DSL.

Where an employee is suspected of accessing illegal or inappropriate sites, or has been accused of inappropriate conduct via electronic media, the Staff Code of Conduct and Positive Smiles disciplinary procedures apply. An immediate referral should be made to the DSL (or Deputy DSL), who will inform the Directors and begin an investigation under Positive Smiles' agreed procedures, referring to adult social care and, where required, the DBS. An early decision needs to be made as to whether the incident should be reported to the Police.

Depending on the circumstances, a decision may be made to suspend an employee while the investigation is ongoing. The Directors will provide support and advice throughout. Actions might include escorting the employee to their workstation to collect personal belongings only. Employees may be asked to hand over all keys, access cards and Positive Smiles equipment, including mobile phones, tablets and cameras. The employee's access to Positive Smiles systems should be suspended pending the result of the investigation. It may be appropriate to advise the employee not to contact any staff or participants directly.

Signed by the Director



01/08/2026