APPEER Connecting autistic girls and women

ICT, E-Safety Policy and Communications Policy V1.9

1. Purpose

The purpose of this policy is to ensure that all ICT systems, online platforms, and virtual support tools used by APPEER CIC are safe, secure, and used responsibly. This policy provides rules and guidance for the safe use of digital tools, online communications, and virtual service delivery.

This policy aims to protect:

- Beneficiaries, including young people and vulnerable adults
- Staff, volunteers, and contractors
- Organisational data and systems

2. Scope

This policy applies to:

- All APPEER CIC staff, volunteers, contractors, and partners
- All ICT equipment and systems, including computers, laptops, tablets, phones, and servers
- All software, applications, online platforms, social media, and virtual support tools used for APPEER CIC activities
- All online and virtual communications with beneficiaries, including video calls, email, messaging, and collaborative platforms

3. Policy Principles

APPEER CIC is committed to:

- Safe use of ICT systems in line with relevant legislation, including the UK GDPR, Data Protection Act 2018, and safeguarding regulations
- Protecting participants from harm online, including exposure to inappropriate content, cyberbullying, or exploitation
- Maintaining confidentiality of personal and sensitive data during virtual support
- Promoting responsible digital behaviour among staff, volunteers, and participants

Registered Office: Steward House, 14 Commercial way, Woking, Surrey, GU21 6ET **appeer.org.uk** Tel: 07861 696542 **Company No: 12271361** VAT No:443494482

4. Policy Owners and Monitoring

The CEO and the Designated Data Protection Officer (DPO) are responsible for this policy and its implementation. ICT systems and online activity are regularly monitored to ensure compliance with this policy and oversight from the Board of Directors.

4.1 Policy Review

The policy is reviewed annually, or sooner if there are changes in legislation, technology, or organisational needs. Feedback and lessons learned from incidents will inform policy updates.

5. Responsibilities to uphold this policy

5.1 Staff and Volunteer Responsibilities

- Follow all ICT, e-safety, and data protection policies.
- Use organisation-provided accounts and devices for work purposes only.
- Protect login credentials and devices; do not share passwords.
- Do not use personal devices during sessions. In emergencies, staff may use personal devices away from the session room when agreed with line management.
- Report any ICT or e-safety incidents immediately to the Data Protection Officer (DPO).
- Complete mandatory ICT and e-safety training during induction and annual refresher sessions.

5.2 Management Responsibilities

- Ensure ICT systems are secure, updated, and maintained.
- Monitor compliance with e-safety and virtual support protocols.
- Provide guidance and training for staff, volunteers, and service users.

6. Safe Use of Technology

- Devices must have up-to-date antivirus software and firewalls enabled
- All software and applications must be approved by the APPEER CIC CEO and DPO
- Personal devices should only be used for work with prior authorisation and must follow organisational security measures
- Data must be stored securely, encrypted when transferred using the approved transfer procedure, and access restricted where appropriate.

7. Virtual Support Safety

7.1 General Guidelines

- Only use secure platforms approved by APPEER CIC for video calls, messaging, or collaborative work
- Always obtain consent from service users or their guardians before virtual sessions
- Do not use personal social media messaging apps or other personal communication methods to communicate with beneficiaries
- Maintain professional boundaries at all times during virtual support

7.2 Conduct During Virtual Sessions

All staff must:

- Ensure sessions are conducted in private settings free from interruptions
- Keep records of virtual sessions where appropriate, while respecting confidentiality – ensuring consent is provided where appropriate
- Dress professionally and ensure backgrounds are appropriate for each session

8. Online Behaviour and Safeguarding

All staff must:

- Not share confidential or sensitive information publicly or with unauthorised individuals including unrelated staff or volunteers
- Prevent to the best capabilities and report cyberbullying, harassment, or exploitation immediately
- Monitor the online safety of service users during sessions; assign a moderator for each session to provide assistance where needed
- Follow all safeguarding procedures if any concerns arise report immediately to the Designated Safeguarding Lead at DSL@Appeer.org.uk

9. E-Safety and Safeguarding in Online Sessions

E-safety is a key part of our support for young people and is applied according to the nature of the sessions they attend. Appeer uses secure virtual accounts for all online Sessions, which require additional safeguarding measures due to participants' access to the internet and online content. Programme Managers are responsible for ensuring that appropriate e-safety measures are activated and verified prior to each session. The specific measures will depend on the activity, the age group of participants, and the level of parental or carer involvement.

9.1 Responsibilities and Limitations

Due to the nature of virtual support we understand that:

- Interactive Sessions cannot guarantee that unsuitable material will never appear

- Controls and terms and conditions are in place to reduce risk, but participants—including parents/carers and staff—have an increased responsibility

Appeer cannot accept liability for:

- Material accessed by families outside Sessions
- Consequences of internet use outside Sessions
- Contributions or visibility of other participants

9.2 Safeguarding Measures

Appeer takes all reasonable precautions to ensure that online sessions are safe, secure, and supportive for all participants. Safeguarding measures are designed to minimise risks associated with internet use and online interactions, while promoting a positive and inclusive environment.

These measures cover session planning, participant verification, parental supervision, secure access, and staff responsibilities, and are adapted according to the age, needs, and engagement level of participants. Programme managers and facilitators are responsible for implementing and monitoring these measures for every session.

9.3 Our E-Safety and Safeguarding measures include:

Planned timetable and fully trained facilitators:

Sessions for autistic girls and women are delivered according to a planned timetable by fully trained facilitators. All facilitators are recruited through our safe recruitment process, have completed a full induction programme, and received comprehensive safeguarding training.

Restricted access:

Session links and access details are only shared with verified families who have completed Appeer Sign Up forms and accepted the terms and conditions. Online sessions are for Appeer participants only, and, where appropriate, their parents/carers.

Parental supervision:

Parents/carers must remain in the room or nearby (line of sight/able to hear) for girls' sessions.

- For Teen Sessions, parents/carers must stay locally and be reachable by phone.
- Young people should not be present during Parent/Carer Sessions to prevent exposure to content that may not be appropriate for them.

Secure access:

- Meeting IDs and passwords are only sent to verified participants.
- Attendees are not permitted to share credentials with anyone else.
- Presenters will keep video on at all times to ensure participants can see who they are speaking to.
- Staff will verify participant names and identities against attendance lists and may remove anyone whose identity cannot be verified.

Behaviour Reminders and Moderation:

- Staff and families are reminded of their responsibilities and expectations for appropriate behaviour before each session.
- Each session will have a responsible moderator to monitor participant activity and intervene if risks arise.
- Participants are directed to this and other relevant policies for guidance, and any safeguarding concerns are reported promptly according to procedures.

Presenter verification:

- All presenters are required to keep their video on during sessions so participants can clearly see who they are interacting with.
- Staff will verify the names and identities of all participants against the attendance list before allowing access.
- The decision to permit entry is at the sole discretion of Appeer staff, using their professional judgment.
- Any participant whose identity cannot be verified will be removed from the session immediately.

Behaviour reminders:

- Staff and families reminded of responsibilities and behaviour before each Session
- Participants directed to relevant policies

Online Behaviour & Safeguarding – Quick Guide for Staff and Volunteers
• **Keep it private:** Never share confidential info with unauthorised people. • **Stop abuse:** Report cyberbullying, harassment, or exploitation immediately. • **Stay alert:** Monitor service users during virtual sessions and act if risks appear.

- **Assign a moderator:** Each session must have one responsible moderator.
- **Follow procedures:** Report any safeguarding concerns without delay.

10. ICT-Related Communication

10.1 Internal & External Tools

- Secure Microsoft accounts for internal/external communication
- Microsoft Office and collaborative tools for document creation, sharing, and storage
- COACHA for participant databases, event bookings, and session communications

10.2 Communication with Beneficiaries

- Social media: Facebook, Instagram, LinkedIn
- Website
- Mailchimp newsletter
- COACHA– participant database - emails
- Customer Records Management system (Capsule)

Note: Beneficiaries only added to newsletters upon request

11. ICT / Phone Supervision During Activities

In-person activities:
Staff supervise young people using online platforms or mobile technology

Virtual activities:
Parents/carers responsible for supervision

Age-appropriate use:

Supervisors ensure all accessed content is suitable for the child's age and understanding

Addressing concerns:

Inappropriate content removed immediately; concerns reported to programme leads and parents/carers as needed

12. Incident Reporting

- All ICT, e-safety, or virtual support incidents must be reported immediately to the DPO

- Reports submitted to Data Protection Lead and safeguarding team where appropriate
- Incidents investigated, logged, and corrective action implemented

13. Training and Awareness

- Mandatory ICT and e-safety training for all staff, volunteers, and contractors
- Annual refresher training or when significant changes occur
- Guidance materials available for staff, volunteers, and service users

14. Compliance and Disciplinary Action

- Breaches of this policy may result in disciplinary action, up to and including termination
- Serious breaches may also result in legal action under UK law

ICT, E-SAFETY, COMMUNICATIONS AND VIRTUAL SUPPORT POLICY V.1.9	
Summary:	This policy sets out Appeer's guidance and procedures for the use of ICT, including ICT hardware and software, electronic communications (such as email and social media), and our commitment to e-safety. It also outlines how we plan and deliver online sessions to ensure the safety, protection, and support of both our staff and beneficiaries.
Policy Owner:	Annaliese Boucher
Author:	Annaliese Boucher
Target Audience:	All staff, beneficiaries
Approved and Ratified By:	Cathryn Jagger 09/02/2025
Version Date:	09.02.26
Next review Date:	09.02.27

Change Record				
Date	Author	Version	Pages	Reason for change
10th April 2020	Jo Dilworth, CEO	1.1	4-5 changes throughout document	To accommodate Zoom sessions with girls from groups and with parents/carers
8th October 2020	Jo Dilworth, CEO	1.2	Changes throughout	To accommodate changes

25th November 2020	Jo Dilworth	1.3	Changes throughout	To accommodate use of Capsule CRM for client data
22nd June 2021	Jo Dilworth, CEO	1.4	Changes throughout	To accommodate new Programmes
6th January 2022	Jo Dilworth, CEO	1.5	Changes due to new generic Appeer Services application form and addition of women's Programme	To accommodate changes
1st February 2024	Jo Dilworth, CEO	1.6	Changes due to new phone and communications.	To accommodate changes To communications.
20th March 2024	Jo Dilworth, CEO	1.7	Throughout	To accommodate change
1st March 2025	Annaliese Boucher, Business Manager	1.8	Throughout	Change in post holders
9th February 2026	Annaliese Boucher, Interim CEO	1.9	Throughout	Change in role, clarifications and legislation updates.

ICT & E-Safety Practical Checklist

For Staff and Volunteers

- ✓ Use only organisation-provided accounts and devices for work
- ✓ Keep passwords and login details private and secure
- ✓ Never use personal devices during sessions; if necessary, move away from the session room
- ✓ Report any ICT or e-safety incidents immediately to the DPO
- ✓ Complete mandatory ICT and e-safety training on induction and annually
- ✓ Follow all ICT, e-safety, and data protection policies

For Management

- ✓ Ensure all ICT systems are up-to-date, secure, and maintained
- ✓ Monitor staff compliance with e-safety and virtual support protocols
- ✓ Provide clear guidance and training on ICT, e-safety, and data protection
- ✓ Act promptly on any reported incidents or concerns

Registered Office: Steward House, 14 Commercial way, Woking, Surrey, GU21 6ET **appeer.org.uk** Tel: 07861 696542 **Company No: 12271361** VAT No:443494482