APPEER Connecting autistic girls and women

Data Protection Policy V1.9

APPEER COMMUNITY INTEREST COMPANY (CIC)

In this policy, the following definitions apply:

"Appeer"	Appeer Community Interest Company ("We, our, us")
"Session"	An event organised by Appeer or a contracted third-party service provider, either as a one-time occurrence or part of a programme.
"Programme"	A series of sessions offered during a specific period, including online sessions, scheduled at predetermined times and locations, and conducted either by Appeer or a third-party service provider contracted by Appeer.
"Participant" and "Adult Participant"	A person registered with Appeer and/or who has, is or will attend an Appeer activity or programme
"Data controller"	A person, company, or other body which decides the purposes and methods of processing personal data
"Data processor"	A person, company, or official entity that processes personal data on behalf of a data controller.
"Data subject"	A data subject refers to an individual whose personal information is being collected, processed, or stored.
"Personal data"	Personal data refers to information that can identify an individual, such as a name, identification number, address, biometric data, etc.
"Processing"	Any activity relating to personal data which can include collecting, recording, storing, amending, disclosing, transferring, retrieving, using or destruction.
"Third party"	A natural or legal person, public authority, agency, or body other than the data subject, controller, processor, and those authorised to process personal data under the direct authority of the controller or processor.

APPEER *Connecting autistic girls and women*

Data Protection Policy Statement

This Data Protection Policy outlines our commitment to safeguarding the information we collect, use, transfer, and store. It includes the personal data and special category data we may collect of our employees, participants, customers, and suppliers. The policy is established in compliance with applicable data protection legislation, including the Data Protection Act 2018 and the UK General Data Protection Regulation (UK GDPR), along with other relevant regulations and guidelines.

Scope of the Data Protection Policy

Our Data Protection Policy and related procedures and guidance apply to all employees, volunteers, beneficiaries, and anyone else with or representing Appeer Community Interest Company (CIC). Adherence to this policy is mandatory for all employees, volunteers, and any third parties instructed to work on behalf of Appeer Community Interest Company (CIC) as part of their individual contractual agreement.

The purpose of this policy is to:

- ✓ Evidence our commitment to data protection
- ✓ Outline our principles and procedures for collecting, storing and managing data
- ✓ Outline security measures for personal data, protecting it from unauthorised access, loss, or damage.
- ✓ Set out the basis on which we will process any personal data we collect from you, that you provide to us, or that comes to us via someone else
- ✓ Outline the types of personal data we collect and purposes to process
- ✓ Outline how data is stored and managed
- ✓ Inform individuals of their rights and freedom regarding their personal data

Data Protection Policy management and review

This Data Protection policy and associated data protection procedures are reviewed annually, or, where necessary, revised by the Data Protection Officer (DPO) at an earlier stage. Review and amendment are overseen and approved by the CEO and board of directors.

Data Protection Officer (DPO)

Under the UK GDPR, organisations that regularly process personal data must appoint a Data Protection Officer (DPO). The DPO is responsible for ensuring compliance with data protection policies and legal requirements and promoting effective data protection practices within the organisation.

Appeer Community Interest Company (CIC) has appointed Annaliese Boucher, Business Manager, as the designated Data Protection Officer (DPO). For further information regarding this policy, please contact the email: **DPO@appeer.org.uk**

Implementation of Data Protection Policy and Procedures

APPEER CIC ensures the effective implementation of its Data Protection Policy and procedures by assigning clear responsibilities, providing training, and regularly reviewing compliance to protect personal data. We provide the following to ensure that the policy is effective:

1. **Clear Roles and Responsibilities**

- A designated Data Protection Lead oversees compliance and acts as the main point of contact for data protection matters.
- All staff, volunteers, and contractors are responsible for handling personal data securely and in line with policy requirements.
- Managers ensure their teams understand and follow the data protection procedures in daily operations.

2. **Comprehensive Training and Awareness**

- All new staff and volunteers receive data protection training during induction.
- Annual refresher sessions and updates are provided to maintain awareness and address any legal or procedural changes.
- Targeted training is given to those handling sensitive or special category data.

3. **Documented Procedures**

- Written procedures outline how personal data should be collected, stored, shared, and deleted.
- Procedures for subject access requests, data breaches, and data retention are in place and regularly tested.
- Staff have access to up-to-date documentation through the internal policy library or shared drive.

4. **Regular Monitoring and Review**

- The Data Protection Lead conducts periodic audits to assess compliance with policy and identify areas for improvement.
- Policy and procedures are reviewed annually or sooner if legislation or organisational needs change.
- Findings from reviews are reported to senior management, with corrective actions tracked to completion.

5. **Data Security Measures**

- Technical measures such as password protection, encryption, secure file sharing, and access controls are enforced.

- Physical measures include locked storage, controlled access to premises, and secure disposal of paper records.
- Systems are regularly updated to reduce cyber risk and maintain confidentiality, integrity, and availability of data.

6. Incident and Breach Management

- A Data Breach Procedure ensures that any incident is reported, investigated, and resolved promptly.
- All staff are trained to recognise and report potential data breaches immediately.
- Serious breaches are escalated and, where required, reported to the Information Commissioner's Office (ICO) within statutory timescales.

7. Transparency and Accountability

- A public Privacy Notice outlines how APPEER CIC collects, uses, and protects personal data.
- Data processing agreements are maintained with all third parties handling data on APPEER's behalf.
- Records of Processing Activities (ROPA) are maintained to demonstrate compliance with UK GDPR.

8. Continuous Improvement

- Feedback from audits, incidents, and staff input informs updates to procedures.
- Best practices are reviewed regularly to align with ICO guidance and sector standards.
- A culture of privacy and data responsibility is promoted throughout the organisation.

Processing personal data

Within this policy and associated Appeer Community Interest (CIC) data protection guidance, we define 'personal data' according to the UK GDPR guidelines definition below.

"any information relating to an identified or identifiable natural person 'data subject'; an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person" – UK GDPR (2018)

Key Principles of Data Protection

In accordance with Article 5 of the UK GDPR, we are committed to processing all data in alignment with data protection legislation.

Appeer Community Interest Company (CIC) adheres to the following key principles of UK GDPR:

Key Principles	Description
Lawfulness, fairness and transparency	**Lawful:** Data subjects are informed on what processing will be done. **Fair:** Ensuring data is processed only as described by the data subject. **Transparent:** Ensuring processing meets the test described in GDPR.
Purpose Limitation	Ensuring data is collected for the explicit, specific and legitimate purposes and not further processed in a manner that is incompatible with those purposes.
Data Minimisation	Data is restricted to what is necessary in relation to the purposes specified.
Accuracy	Data is accurate and maintained. Necessary steps are taken to review, rectify or delete where necessary without delay.
Storage limitation	Data must be kept in a form that permits identification of data subject for no longer than is necessary for the purposes for which the personal data is processed.
Integrity and confidentiality	Data must be processed using the appropriate technical or organisational measures to ensure appropriate security, including protection against unauthorised or unlawful processing and accidental loss, destruction, or damage.

Accountability	The organisation is responsible for complying with UK GDPR and must be able to show compliance if asked to do so.

Our commitment to the key principles of UK GDPR

Appeer Community Interest Company (CIC) will provide the following information to any individual that is subject to data control or processing.

- ✓ The identification of the data controller
- ✓ The purposes for which the data is being processed
- ✓ Any anticipated disclosures of personal data to third parties
- ✓ The expected duration for which the data will be retained
- ✓ Any other relevant information that may be important to the data subject.

Lawful basis for processing data

Under Article 6 of the UK GDPR, an organisation must have a lawful reason for processing personal data. Appeer Community Interest Company (CIC) will only process personal data where one or more of the basis can be applied.

Lawful basis	Description
A Consent basis	✓ A consent basis where data subjects are given the choice and control over their personal data. ✓ Consent must be clear, specific, and separate from terms and conditions, with individual consents obtained for different actions ✓ It should be easy for individuals to withdraw consent at any time. ✓ Consent should not be a prerequisite for accessing any Appeer services.
Contract	✓ The purpose of processing data is necessary to successfully fulfilling a contractual obligation. ✓ The minimum reasonable amount of data is processed in order to provide a service.
Legal Obligation	✓ Processing is necessary to comply with common law or a statutory obligation
Vital Interests	✓ Limited basis, only justified to protect the vital interests of the data subject in emergency situations where not doing so may result in threat to life. ✓ Where data subjects are incapable of giving consent.
Public task	✓ 'in the exercise of official authority' ✓ To perform a specific task in the public interest that is set out in law.
Legitimate interests	✓ A specified interest that is justifiable

	✓ Reasonable processing with minimal impact on the individuals privacy. ✓ Fair balance between legitimate interest against individual interests, rights and freedoms.

Special category data

Under UK GDPR Article 9, 'special category data' refers to personal information that reveals:

- Racial or ethnic origin
- Political opinions
- Religious or philosophical beliefs
- Trade union membership
- Genetic data
- Biometric data used for unique identification
- Health information
- Details about sex life or sexual orientation

Lawful Basis for Processing Special Category Data

To lawfully process special category data, the following must be satisfied:

1. There must be a clear lawful basis under Article 6, UK GDPR.
2. The processing must meet one or more conditions under Article 9, UK GDPR.

Note: Article 9 conditions include, but are not limited to, explicit consent, employment obligations, vital interests, legal claims, health or social care purposes, public interest, and legitimate activities by non-profit organisations.

How we collect data

Appeer Community Interest Company (CIC) collects personal data in the following ways for the explicit purposes stated above.

Data Subject	Collection method	System
Participants	Online booking system	COACHA Internal systems (Google Drive)
Employees	Staff HR forms (physical and electronic) manual entry onto systems. Staff surveys/ questionnaires	Safe HR Internal systems (Google Drive) Bright pay
Funders	Direct interactions or forms	Capsule Internal systems (Google Drive)
Contractors/services	Direct interactions or forms	Capsule Internal systems (Google Drive)

Data storage

Appeer Community Interest Company (CIC) Stores data securely, using the following data management systems.

Data Security

Our data security protocols are established to safeguard against unauthorised or unlawful processing and prevent accidental loss, destruction, or damage to sensitive information. Our security measures include the following safeguards, but are not limited to:

- Secure storage of physical documents (lockable storage)
- Access control (restricted access/ password/passcode restricted)
- Access control points (restricted areas/ no public access/ lockable rooms)
- System Password/ Passcode protection
- Regular risk assessment
- Encrypted data security (asymmetric and symmetry encryption)
- Secure Data Transfer Protocol
- System Backing Up
- Secure wireless protocols
- Regular system updates
- Password protocols
- Remote access controls

Data Protection Impact Assessment (DPIA)

Appeer Community Interest Company (CIC) will conduct an annual Data Protection Impact Assessment (DPIA) for any special category data it processes, in compliance with data protection laws, including the UK GDPR and DPA 2018. This assessment will help Appeer CIC identify and minimize data protection risks, understand potential harms to individuals' rights and freedoms related to its data handling practices, and implement strategies to mitigate those risks.

Data retention and disposal

All data processed by Appeer Community Interest Company (CIC) in accordance with operational requirements is governed by the Data Retention and Disposal Policy. This policy outlines the retention periods for various types of data and specifies the appropriate methods for disposing of them.

When personal data is no longer needed, it will be securely disposed of following the established retention schedule. Appeer Community Interest Company (CIC) will not retain personal data longer than necessary for its intended purpose. This approach minimises the risk of data becoming inaccurate, outdated, or irrelevant, ensuring we can justify its retention.

Monitoring data retention and disposal

Data collection will be retained for five years following the last activity as part of our monitoring and compliance. After this period, personal data will be anonymised, and all identifiable information will be securely disposed of in accordance with our Data Retention and Disposal Policy.

Data retention schedule

Data type	Retention schedule	Disposal method
Participant records (Name, DOB, contact details, medical info, EHCPs, progress reports)	5 years from last date of contact (or until participant reaches 25, whichever is later, for safeguarding purposes)	Secure shredding of physical documents; secure deletion of electronic records
Employee records (HR files, payroll, appraisals, contracts)	5 years after employment ends (or longer if required for pension/insurance purposes)	Secure shredding of physical documents; secure deletion of electronic records
Financial records (Invoices, remittance, receipts)	7-10 years (for HMRC compliance)	Secure shredding of physical documents; secure deletion of electronic records
Education provider records (Contacts, invoices, communications)	7 years	Secure shredding of physical documents; secure deletion of electronic records
Risk assessments & incident reports	10 years (or as long as relevant for safeguarding/legal purposes)	Secure shredding of physical documents; secure deletion of electronic records
Funder and contractor records	7 years	Secure shredding of physical documents; secure deletion of electronic records
Staff surveys/questionnaires	3 years	Secure shredding of physical documents; secure deletion of electronic records

Consent forms	Duration of the relevant activity + 3 years	Secure shredding of physical documents; secure deletion of electronic records

Sharing and Transferring Data to Third Parties

Data Subject Requests

You have the right to request that your personal data be transferred to a third party. We will consider such requests in line with your rights under UK GDPR, ensuring that transfers are secure and lawful.

Sharing Data Without Your Consent

In specific situations, we may process or share special category data without your explicit consent. These situations include:

- When necessary to fulfil legal rights and obligations.
- When essential to protect vital interests of yourself or another person who is physically or legally unable to give consent.
- When you have made the data public.
- When processing is necessary for the establishment, exercise, or defence of legal claims.

Who We May Share Data With

To carry out our contractual obligations and meet the needs of each participant, we may share relevant data with:

- **Internal staff**: To enable them to undertake their roles effectively and provide appropriate support to participants.
- **External or contracted staff:** To support them in delivering services and fulfilling contractual obligations.
- **Surrey Children's Services and other statutory services:** This includes local and national agencies, such as schools, where they are involved in the care of a child or vulnerable adult, or in cases of safeguarding concerns.
- **Supervisors:** During supervision sessions, relevant data may be shared to ensure quality and compliance with safeguarding and professional standards.

Confidentiality and privacy

We require those staff and organisations to keep your personal data confidential and secure and protected in accordance with the law and our policies. They are only permitted to process your data for the lawful purpose for which it has been shared and in accordance with our instructions.

We do not send your personal data outside the European Economic Area when stored on our own systems.

APPEER Connecting autistic girls and women

Data Breaches procedures

In the event of a data breach, we will proactively activate our data breach plan to effectively manage and mitigate the impact of the incident. We are committed to taking the following constructive steps:

Steps	Action
Step One: Assess scope and impact of breach	Identify the data, system, or individual that has been affected and assess the impact of the breach.
Step two: Containment of the breach	Take immediate action to minimise further damage and prevent further access. For example; changing passwords, or amending access controls.
Step three: Investigate circumstances	Carry out a comprehensive investigation to understand how the breach happened and identify any vulnerabilities.
Step four: Implement remediation measures	Strengthen security measures, or fix vulnerabilities.
Step five: Provide support and assistance	Provide assistance to those affected.

Reporting a breach to the Information Commissioner's Office (ICO)

If a breach is likely to result in a risk to the rights and freedoms of individuals, we will inform the Information Commissioner's Office within 72 hours and follow advice given.

Your Data Subject Rights

Under the Data Protection Act 2018, individuals have the rights regarding how their data is used, stored, and managed.

Your rights under data protection law:	
Rights to access	The right to request a copy of the personal data which we hold about you
Right to rectification	The right to request that we correct any personal data if it is found to be inaccurate or out of date
Right to erasure	The right to request your personal data is erased where it is no longer necessary to retain such data
Right to withdraw consent	The right to withdraw your consent to the processing at any time, where consent was your lawful basis for processing the data
Right to restriction of processing	The right, where there is a dispute in relation to the accuracy or processing of your personal data, to request a restriction is placed on further processing
Right to object to the processing of data	The right to object to the processing of personal data (where applicable, i.e. where processing is based on legitimate interests (or the performance of a task in the public interest/exercise of official authority), direct marketing and processing for the purposes of scientific/historical research and statistics
Right to data portability	The right to request that we provide you with your personal data and where possible, to transmit that data directly to another data controller (known as the right to data portability) where applicable, i.e. where the processing is based on consent or is necessary for the performance of a contract with the data subject and where the data controller processes the data by automated means

How to make a data subject request

Everyone has the right to request information about the data we hold on them, including requests to exercise their rights under the Data Protection Act of 2018. To start this process,

individuals should submit their requests in writing, addressed to the Data Protection Officer. Please outline your request clearly and use the contact details provided below:

C/O The Data Protection Officer
Appeer Community Interest Company (CIC)
Steward House
14 Commercial way
Woking
Surrey
GU21 6ET

How to make a complaint regarding Data Management

If you would like to file a complaint regarding our data management, please get in touch with the Data Protection Officer (DPO) to initiate the formal complaints procedure. The DPO will respond to your complaint within 10 working days. If an investigation is necessary, the DPO will carry it out and provide the findings and response within 28 days of receiving the complaint.

If you feel your complaint has not been satisfactorily resolved, you have the right to escalate your complaint to the Information Commissioner's Office.

Information Commissioner's Office
Wycliffe House, Water Lane
Wilmslow, Cheshire, SK9 5AF
Helpline number: 0303 123 1113 / ICO website: https://www.ico.org.uk

Further Appeer Community Interest Company (CIC) policies and guidance

- Data Security Policy
- Data Management Policy
- Data Retention and Disposal Schedule
- ICT, E-Safety and virtual support Policy
- Privacy Policy

Data Protection Policy Version No: 1.9	
Summary:	**Policy outlines our commitment to safeguarding the information we collect, use, transfer, and store.**
Policy Owner:	**Annaliese Boucher**
Author:	**Annaliese Boucher**

APPEER *Connecting autistic girls and women*

Target Audience:	**Beneficiaries and staff**
Approved and Ratified By:	**Jo Dilworth**
Version Date:	**19th March 2026**
Date of issue:	**19th March 2026**
Next Review Date:	**20 March 2027 or earlier if changes in programmes or legislation.**

Change Record				
Date	Author	Version	Page/s	Reason for Change
10th April 2020	Jo Dilworth, Director & DSL	1.1	4 or 5 changes throughout the document	To accommodate Zoom sessions with girls from groups and with parents/carers.
8th October 2020	Jo Dilworth, CEO & Girls Programme Lead	1.2	Changes throughout	To accommodate changes for new girls' and parent/carer sessions from October 2020
25th November 2020	Jo Dilworth, Director & CEO	1.3	Changes throughout.	To accommodate use of Capsule CRM for client data.
22nd June 2021	Jo Dilworth, Paige Sinkler, Cathryn Jagger, various positions	1.4	Changes throughout	To accommodate new programmes
6th January 2021	Jo Dilworth, CEO	1.5	Changes due to new generic Appeer Services application form and addition of women's programme	To accommodate changes to application form and addition of women's programme
21 September 2022	Paige Sinkler, Co-CEO (Management) and DC	1.6	Minor formatting changes throughout and major change on p7	To align with other policies' format, and to change the identity of Data Processor.
20 March 2024	Jo Dilworth, CEO	1.7	Changes throughout	To accommodate changes in role and Coacha

20 March 2025	Annaliese Boucher, Business Manager (DPO)	1.8	Clarifications	Change in role holder additional procedures and processes.
13th January 2026	Sarah Nolan	1.8	Throughout	Staffing changes
19th March 2026	Annaliese Boucher, CEO (DPO)	1.9	Review – no changes	