APPEER Connecting autistic girls and women

Data Privacy Policy V1.8

Participants, Clients and Suppliers

APPEER COMMUNITY INTEREST COMPANY (CIC)

Purpose of the Data Privacy Policy

This Data Privacy Policy explains how Appeer Community Interest Company (CIC) manages personal data, ensuring transparency and empowering individuals to make informed decisions about their information. It outlines our commitment to safeguarding the data we collect, use, transfer, and store, including both personal and special category data from participants, clients, or suppliers.

Data Protection review and monitoring

This Data Privacy Policy and related data protection processes are reviewed annually. If necessary, the Data Protection Officer (DPO) may conduct earlier revisions. The CEO and board of directors oversee and approve these reviews and amendments.

Our Legal and Regulatory duty

This Data Privacy Policy is established in compliance with applicable data protection legislation, the Data Protection Act 2018 and the UK General Data Protection Regulation (UK GDPR,2018), along with other relevant regulations and guidelines of good practice.

What is meant by participant

Any individual registered with Appeer and/or who has, is or will attend an Appeer activity or programme in some capacity.

What is meant by client

A client is anyone, including organisations or individuals like caregivers of youth under 18, who obtain services from Appeer Community Interest Company (CIC). This may change if caregivers are authorised to act for participants over 18. Schools and local authorities are also considered clients when receiving services.

What is meant by supplier

A person or organisation that provides product or services to Appeer Community Interest Company (CIC).

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 *Connecting autistic girls and women*

Named Data Protection Officer (DPO)

Appeer Community Interest Company (CIC) has appointed **Annaliese Boucher** as the designated **Data Protection Officer (DPO).** For further information regarding this policy or to address any queries, please email annaliese@appeer.org.uk.

What is Personal data?

Appeer Community Interest Company (CIC) defines personal data as any information that relates to an identified or identifiable natural person, whether directly or indirectly. This includes information such as names, addresses, email addresses, phone numbers, dates of birth, physical characteristics, photos, video recordings, IP addresses, and online identifiers. All of these are considered personal data.

What is Special Category data?

UK GDPR article 9, refers to 'special category data' as personal information that reveals a person's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, and biometric data used for unique identification. It also includes data related to an individual's health or details about their sex life or sexual orientation which may be collected periodically for specific monitoring or project activities.

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.

Data Collection and Management

See below table in reference to the information we may collect and how.

Data subject	Data collected	Collect method	Purpose
Participants	Name, DOB, Contact details Medical details Education setting details (where appropriate) Special category data (race,gender,age, disability etc.) Risk assessments, care plans and EHCP (Where appropriate) Progress and attainment Images, testimonials, information for payment for service, engagement records.	COACHA Internal systems (Google Drive) surveys/ questionnaires Emails, letters, telephone log.	• Maintain accurate Participant records • Contractual obligations and internal monitoring and evaluations • Legal obligations related to Health and Safety • Equality, Diversity and Inclusion (EDI) • Minimum service requirements • Marketing and Communications
Clients	Company details, point of contact, purchase history, financial information (for invoices), feedback, correspondence, engagement.	COACHA Internal systems (Google Drive) Capsule CRM	• Maintain accurate records • Contractual obligations and internal monitoring and evaluations
Suppliers	Company details, point of contact, purchase history, financial information (for purchases/invoices) feedback, correspondence, engagement.	COACHA Internal systems (Google Drive) Capsule CRM	• Maintain accurate records • Contractual obligations and internal monitoring and evaluations

Keeping your Data Secure

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 minimise 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 sharing

Appeer Community Interest Company (CIC) will never share your information with a third party without your explicit consent. However, we may not require your consent to process your data in specific situations. These situations may include the following cases:

- When it is necessary to fulfil rights and obligations under the law.
- When it is essential to protect your vital interests or those of 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.

Sharing data outside of the UK

Appeer Community Interest Company (CIC) is committed to protecting your privacy and ensuring the security of your personal information. As part of this commitment, we do not share any data with third parties or organisations located outside of the United Kingdom. This policy helps us maintain strict control over how your information is used and safeguarded.

Transferring data

Individuals have the right to request the transfer of their personal data under Article 20 of the General Data Protection Regulation (GDPR), which covers data portability. This transfer should be technically feasible and free from any barriers, including legal, technical, or financial obstacles. We will only transfer data, whether by request or to fulfil legal rights and obligations, in accordance with our established safe data transfer protocols.

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. Data subject will always be informed on how their data will be used and how long it will be retained for its purpose.

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.

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 Connecting autistic girls and women

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

Data Privacy Policy Version No: 1.8	
Summary:	It outlines our commitment to safeguarding the data we collect, use, transfer, and store, including both personal and special category data from participants, clients, or suppliers.
Policy Owner:	Annaliese Boucher, Samantha Emmerson (CEO)
Author:	Annaliese Boucher (Business Manager)
Target Audience:	Beneficiaries, Staff, Clients and suppliers
Approved and Ratified By:	Samantha Emmerson
Version Date:	20th March 2025
Date of issue:	20th March 2025
Next Review Date:	19th March 2026 or earlier if changes in programmes or legislation.

20 March 2024	Jo Dilworth, CEO	1.7	Changes throughout	To accommodate changes in role and Coacha
15 March 2025	Annaliese Boucher	1.8	Changes throughout	