APPEER Connecting autistic girls and women

Secure Data Transfer Protocol V1.0

1. Purpose

To ensure all personal and confidential information transferred by APPEER CIC — electronically or physically — is handled securely to prevent unauthorised access, loss, or misuse.

2. Scope

This protocol applies to all staff, volunteers, contractors, and partners who send, receive, or share personal data on behalf of APPEER CIC.

It covers all methods of data transfer, including but not limited to:

- Email
- Cloud storage or file-sharing systems (e.g., OneDrive, SharePoint, Google Workspace)
- Physical media such as USB drives, CDs, or paper files
- Data exchanges with third parties (e.g., partner organisations, funders, external agencies)
- SMS or text messaging used to communicate personal or sensitive information

All transfers must comply with the principles and procedures outlined in this protocol to ensure data is protected, secure, and only shared for legitimate purposes.

3. Principles of Secure Data Transfer

All data transfers must:

- Be lawful, necessary, and proportionate for a defined purpose.
- Use the most secure method available.
- Be limited to the minimum data required for the task.
- Be authorised by a manager or Data Protection Lead if data includes special category information.
- Be recorded or logged when appropriate (especially external transfers).

4. Approved Methods for Secure Data Transfer

1. Email

- Use organisation-approved email accounts (never personal email).

For sensitive or personal data:

- ✓ Use encrypted email attachments (e.g., password-protected Word or PDF files).
- ✓ Share passwords via a separate channel (e.g., phone or text).
- ✓ Double-check recipient addresses before sending.
- ✓ Use "bcc" when emailing multiple recipients to avoid disclosing addresses.

2. Secure File-Sharing Platforms

- Use approved cloud storage systems (e.g., OneDrive, SharePoint with encryption).

- Share files using restricted access links (e.g., view-only or time-limited permissions).
- Revoke access once the task is complete.
- Avoid open or public file-sharing links.

3. Physical Data Transfer

- Only use encrypted USB drives for portable data transfers.
- Keep physical documents in sealed, labelled envelopes and send by recorded delivery or courier if necessary.
- Ensure physical transfers are tracked and logged.
- Confirm receipt by the authorised recipient.

4. Internal Data Transfers

- Use secure internal networks rather than downloading or emailing data unnecessarily.
- Restrict access to relevant team members only.
- Avoid transferring sensitive data through unapproved instant messaging or collaboration tools.

5. Data Transfer Agreements (External Parties)

When transferring data to or receiving data from another organisation:

A Data Sharing Agreement (DSA) or Data Processing Agreement (DPA) must be in place (See APPENDIX A & B)

The agreement should set out:

- ✓ Purpose and lawful basis of data sharing
- ✓ Security measures required by both parties
- ✓ Responsibilities for data breaches or data subject requests

The Data Protection Officer (DPO) must review and approve all external data-sharing arrangements.

6. Data Integrity and Verification

- Before transferring data, verify the recipient's identity and authorisation.
- Confirm that data is accurate, complete, and necessary for the stated purpose.
- After transfer, confirm successful and secure receipt.

7. Incident Management

If a data transfer error occurs (e.g., sent to the wrong person, unencrypted file shared, lost device):

- Report immediately to the Data Protection Lead or manager.
- Follow the Data Breach Response Procedure.
- Do not attempt to delete or recall data without instruction — follow investigation steps.

8. Monitoring and Review

- The Data Protection Officer (DPO) will conduct periodic audits of data transfers.
- Transfer methods and agreements will be reviewed annually or when new systems or partners are introduced.
- Updates will be communicated to staff, and further training provided if needed.

9. Staff Responsibilities

All employees, volunteers, and contractors must:

- Always follow this protocol.
- Complete data protection and cybersecurity training.
- Report any data handling concerns or breaches promptly.

10. Compliance

Non-compliance may result in disciplinary action under APPEER CIC's policies.

11. Monitoring and review of Protocol

APPEER CIC is committed to ensuring that the Secure Sharing Data Protocol remains effective, up-to-date, and compliant with all relevant legislation, including the GDPR and the Data Protection Act 2018.

The Secure Sharing Data Protocol l will be reviewed at least annually, or sooner if required due to:

- Changes in legislation or regulatory guidance
- Lessons learned from breaches or near-miss incidents
- Updates to IT systems, processes, or company procedures

The review will assess:

- The adequacy of the procedures
- The effectiveness of containment and mitigation measures
- Whether staff training is sufficient to ensure awareness of their responsibilities
- Any necessary amendments will be implemented promptly, communicated to all staff, and incorporated into training programmes.

SECURE SHARING DATA PROTOCOL V1.0	
Summary:	Guidance on managing a data breach and internal procedures
Policy Owner:	Annaliese Boucher
Author:	Annaliese Boucher
Target Audience:	staff
Approved and Ratified By:	25th October 2025
Ratified by:	Samantha Emmerson (CEO)
Version Date:	22nd October 2025
Date of issue:	1st November 2025
Next Review Date:	1st November 2026

APPENDIX A: DATA SHARING AGREEMENT (DSA) TEMPLATE

This Agreement is made on [Date]

Between:

1. [Organisation Name & Address] ("Data Provider")
2. [Organisation Name & Address] ("Data Receiver")

Collectively referred to as "the Parties."

1. Purpose of Data Sharing

The purpose of this Agreement is to define the terms under which the Parties will share data for [state purpose, e.g., educational support, research, monitoring student progress]. Data will be shared only to achieve this purpose.

2. Description of Data

The Data Provider will share the following types of data with the Data Receiver:

Data Type	Description	Format	Sensitivity
Example: Student Name	Full legal name	CSV / Excel	Personal Data
Example: Attendance	Daily attendance records	CSV / Excel	Personal Data
Example: Assessment Results	Exam scores and feedback	PDF / Excel	Personal Data

Additional details may be attached as Annex A.

3. Legal Basis

The Parties confirm that the sharing and processing of data will comply with applicable laws, including:

- UK Data Protection Act 2018 / GDPR
- Other relevant legislation: [specify]

The lawful basis for processing is: [Consent / Legal Obligation / Legitimate Interest].

4. Responsibilities of the Parties

Data Provider shall:

- Ensure data is accurate, complete, and up-to-date
- Share only data necessary for the stated purpose

Data Receiver shall:

- Use the data solely for the agreed purpose
- Implement appropriate technical and organisational measures to protect data (encryption, secure storage, access controls)
- Notify the Data Provider immediately in case of a data breach

5. Access and Usage

- Access to the data is limited to authorised staff only
- Data must not be shared with any third party without prior written consent
- Data must not be used for any purpose other than stated in Section 1

6. Retention and Disposal

- Data will be retained until [date / event]
- Upon expiry, data will be securely deleted or anonymized
- Any backups or copies must also be destroyed

7. Audit and Compliance

- Parties agree to cooperate with audits to ensure compliance
- Records of data access and processing must be maintained

8. Liability

- Each party is responsible for compliance with data protection laws within its own organisation
- Any breach caused by negligence will be addressed per legal obligations

9. Amendments

- Any changes to this Agreement must be documented in writing and signed by both Parties

10. Termination

- This Agreement may be terminated by either party with [number] days' written notice
- Termination does not affect obligations to securely dispose of data already shared

11. Signatures

Name & Title	Organisation	Signature	Date
[Name]	Data Provider		
[Name]	Data Receiver		

APPENDIX B: DATA PROCESSING AGREEMENT (DPA) TEMPLATE

This Agreement is made on [Date]

Between:

1. [Data Controller Name & Address] ("Controller")
2. [Data Processor Name & Address] ("Processor")

Collectively referred to as "the Parties."

1. Definitions

- Personal Data: Any information relating to an identified or identifiable individual.
- Processing: Any operation performed on personal data, including collection, storage, use, analysis, disclosure, or deletion.
- Data Subject: Individual whose personal data is being processed.
- Sub-processor: Any third party engaged by the Processor to carry out processing on behalf of the Controller.

2. Subject Matter & Duration

- The Processor will process personal data on behalf of the Controller for the purpose of [describe purpose, e.g., student support, payroll, IT services].
- Duration: From [start date] to [end date or ongoing].

3. Nature & Purpose of Processing

- Nature: e.g., collection, storage, analysis, reporting, communication.
- Purpose: e.g., educational management, staff payroll, IT support.

4. Types of Personal Data & Categories of Data Subjects

Data Type	Description	Data Subjects
Example: Student Name	**Full legal name**	**Students**
Example: Attendance	**Daily attendance records**	**Students**
Example: Contact Info	**Email, phone number**	**Parents & Staff**
Example: Assessment Results	**Exam scores and feedback**	**Students**

5. Processor Obligations

The Processor shall:

1. Process data only according to the Controller's instructions.
2. Implement appropriate technical and organisational measures to protect data (encryption, secure storage, access control).
3. Ensure all personnel handling the data are subject to confidentiality obligations.
4. Notify the Controller without undue delay of any personal data breaches.
5. Assist the Controller in responding to data subject rights requests.

6. Sub-processors

- The Processor may engage sub-processors only with the prior written consent of the Controller.
- The Processor remains fully responsible for the actions of sub-processors.

7. Data Security

- Apply appropriate technical and organisational measures to protect personal data against unauthorized or unlawful processing, accidental loss, destruction, or damage.
- Review and update security measures regularly.

8. Data Breach Notification

- The Processor must notify the Controller within 24 hours of discovering any data breach.
- Provide sufficient details to allow the Controller to meet regulatory obligations.

9. Data Return or Deletion

- Upon termination or expiry of this Agreement, the Processor shall return or securely destroy all personal data.
- Any backups or copies must also be destroyed.

10. Audit & Inspection

- The Controller may audit the Processor to ensure compliance with this Agreement.
- The Processor must provide full cooperation and access to relevant records.

11. Liability

- Each Party is responsible for compliance with data protection laws within its organisation.
- Liability for breaches caused by negligence will follow applicable law.

12. Governing Law

- This Agreement is governed by [UK GDPR / EU GDPR] and relevant local legislation.

13. Signatures

Name & Title	Organisation	Signature	Date
[Name]	Data Controller		
[Name]	Data Processor		