APPEER Connecting autistic girls and women

INTERNAL USE:

Data Breach Policy V1.1

At APPEER Community Interest Company (CIC), we take privacy seriously. We implement all reasonable precautions to protect personal data and actively work to prevent any breaches that could compromise data security or the rights of our beneficiaries, clients, customers, stakeholders, or anyone connected with the company.

1. Purpose

This policy sets out our approach to mitigating the risks associated with data breaches. It is part of our compliance with the General Data Protection Regulation (GDPR) and the Data Protection Act 2018. The policy:

- Establishes clear lines of responsibility for managing data breaches.
- Provides processes for identifying, reporting, and responding to breaches.
- Ensures that any incidents are handled promptly to minimise impact.

2. Scope

This policy applies to **all personal and sensitive data** held by APPEER CIC. It is relevant to everyone associated with the company, including:

- Employees (full-time, part-time, temporary, or casual)
- Consultants, contractors, and freelance workers
- Suppliers and third-party data processors

Anyone storing or processing data on behalf of APPEER CIC must follow this policy to ensure data protection standards are upheld.

Ownership of Policy
The Data Protection Officer is responsible for the monitoring and maintenance of this policy.

For further information or guidance please contact the designated Data Protection Officer at DPO@appeer.org.uk

3. Definition of a Data Breach

A data breach is any incident, event, or action that has the potential to compromise:

- The availability of data
- The integrity of data
- The confidentiality of data
- The security of APPEER CIC's data systems

Data breaches can occur accidentally or deliberately, and both confirmed and suspected incidents are considered breaches under this policy.

Examples of Data Breaches:
For the purposes of this policy, a data breach may include, but is not limited to, the following:

- Unauthorised access or use of data
- Unauthorised modification of data
- Loss of personal or sensitive data
- Theft of personal or sensitive data
- Loss or theft of equipment on which data is stored
- Human error leading to data exposure or compromise
- Attempts to gain access to data or IT systems (successful or failed)
- Defacement of web property or online systems
- Physical incidents, such as a fire, that could compromise IT systems

4. Responsibilities and Reporting

All employees who access, manage, or use data are responsible for reporting any data breach or security incident.

5. Reporting Procedure

Any breach or suspected incident must be reported immediately to the employee's line manager using the Data Breach Reporting Form. (APPENDIX A)
The report should include:

- Full details of the incident or breach
- Date and time of occurrence
- Details of the individuals or data affected
- Description of how the breach occurred
- Details of the person reporting the incident

6. After Hours Reporting

If a data breach or security incident occurs or is discovered outside normal company hours, it must be reported as soon as possible.

7. Compliance

Any violation of this data breach policy may result in disciplinary action in accordance with company procedures.

8. Data Breach Containment and Data Recovery

All necessary steps must be taken immediately to minimise the impact of any data breach or security incident. The process of containment should begin with an initial assessment to determine the severity of the incident, assess the potential impact, and identify ways to recover lost data and mitigate further risks.

9. Initial Assessment

When conducting an initial assessment, the following information should be established:

- The data involved in the incident
- Whether the data is sensitive in nature
- The individuals affected by the breach
- Existing security measures protecting the data
- What has happened to the data (e.g., lost, stolen, modified)
- Potential misuse of the data in illegal or inappropriate ways
- Any wider consequences associated with the breach, including reputational, financial, or operational impact

This assessment forms the foundation for containment measures, data recovery actions, and any further investigation required to prevent recurrence.

10. Data Breach Notification

APPEER CIC will determine which individuals or organisations must be notified in the event of a data breach or security incident. Each incident will be assessed on a case-by-case basis, taking into account the following considerations:

- Any contractual notification requirements
- Any legal notification requirements
- The number of individuals affected
- Potential consequences arising from the breach or incident
- Whether notification would help individuals mitigate risks associated with the incident

- Whether notification would assist the company in meeting its legal obligations under the
- GDPR and the UK Data Protection Act 2018
- Whether notifying individuals could prevent unauthorised or illegal use of data
- Whether APPEER CIC must notify the Information Commissioner's Office (ICO)

All data breaches and security incidents, whether suspected or confirmed, must be recorded. This record-keeping helps in analysing the incident and in developing measures to prevent future breaches.

11. The Danger of Notifying Too Many Individuals

In some cases, data security incidents may require the notification of a large number of individuals. However, in other cases, notifying too many individuals could lead to disproportionate inquiries or confusion, potentially creating more risk and disruption.

Whenever we notify an individual, whose personal data has been affected by an incident or breach, the notification will include:

- When the breach occurred
- How the breach occurred
- What data was involved in the breach
- Explicit guidance on how the individual can protect themselves
- A summary of the steps APPEER CIC has already taken to mitigate risks

The goal of this notification is to ensure that affected individuals are well-informed, understand the potential risks, and know what steps to take to protect themselves. We will also carefully consider the scope and scale of notifications to prevent unnecessary confusion or distress.

12. Data Breach Evaluation and Response

Once a data breach or security incident has been contained and necessary steps have been taken to minimise further risks, APPEER CIC will conduct a comprehensive review of the incident. This evaluation will include:

- The cause(s) of the breach or incident
- The effectiveness of the response actions
- Whether changes to existing IT systems, company procedures, or policies are required

Review and Improvement

- All existing protocols will be reviewed to assess their adequacy in preventing future incidents.
- Any necessary amendments to protocols will be identified and implemented as soon as possible to ensure continuous improvement and compliance.

This evaluation is a critical part of ensuring that APPEER CIC remains proactive in preventing future data breaches and continues to meet our obligations under the GDPR and Data Protection Act 2018.

APPENDIX A: Breach Report

Data Breach Report Form

To be completed by employee	
Date of incident	
Date incident was discovered	
Name of the individual reporting incident	
Contact details of the individual reporting incident	
Where the incident occurred	
Description of the incident	

Number of data subjects affected by incident	
Personal data placed at risk by incident	
Description of any actions taken at the point of discovery	

To be completed by the Data Protection Officer	
Name of individual receiving report	
Date report received	
Name of individual the report was forwarded to for action	
Date the report was forwarded for action	

APPENDIX B: Breach Notification Template Letter

Data Breach Notification Letter Template

Dear [Title and Surname],

We regret to inform you that APPEER CIC has identified a breach in our processing system that may have exposed your personal data to unauthorised access by external parties. We have reported this incident to the Information Commissioner's Office (ICO) and, where applicable, to relevant law enforcement agencies. We are also working with cybersecurity experts and legal counsel to minimise any further risk to you.

About the Incident

We understand that you may have questions or concerns regarding this incident. We aim to provide a clear explanation of what happened and why.

Our investigation indicates that the following events contributed to this data security incident:

- [List timeline of events here]
- *DETAILS*

About the Data Involved

We believe the following personal information about you may have been accessed or affected:

- [List details here]
- *DETAILS*

What This Means for You

Based on the type of information involved, the potential consequences for you may include:

- [List details here]
- *DETAILS*

Recommended Actions

To further protect yourself from potential risks associated with this incident, we recommend taking the following steps as soon as possible:

- [List details here]
- *DETAILS*

We sincerely apologise for any inconvenience or concern this incident may cause. APPEER CIC is committed to safeguarding your personal information and will continue to take all necessary steps to prevent any further breaches.

If you have any questions or require further guidance, please contact:

Data Protection Officer

Lindsay Prior

DPO@Appeer.org.uk

07476 156 807

13. Monitoring and Reviewing the Data Breach Policy

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

Monitoring

- All data breaches and security incidents will be recorded and monitored to identify trends, weaknesses, or areas for improvement.
- The effectiveness of response procedures will be reviewed following each incident, including containment, notification, and mitigation actions.
- Key performance indicators (KPIs) or internal audits may be used to assess staff compliance with reporting and response requirements.

Reviewing the Policy

The Data Breach Policy 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 reporting 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 programs.

Continuous Improvement

APPEER CIC will use insights from monitoring and policy reviews to strengthen data security measures, improve staff awareness, and reduce the risk of future breaches.

DATA BREACH POLICY V1.1	
Summary:	**Guidance on managing a data breach and internal procedures**
Policy Owner:	**Lindsay Prior**
Author:	**Annaliese Boucher**
Target Audience:	**staff**
Approved and Ratified By:	**Annaliese Boucher**
Version Date:	**13th October 2026**
Date of issue:	**13th October 2026**
Next Review Date:	**10th August 2027**