Data Security Policy

This policy is for Ambitious about Autism (AaA) and Ambitious about Autism Schools Trust (AaAST) referred to as 'the Charity'.

Purpose and Scope
It is our policy that the data the charity holds shall be appropriately secured, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures. This is in line with the General Data Protection Regulation (GDPR) which comes into effect on 25 May 2018.

This policy applies to all data, both electronic and on paper, and in particular to personal data about service users, supporters, employees and volunteers.

The policy is designed to protect against the consequences of breaches of confidentiality, failures of integrity or interruptions to the availability of that information. In particular it aims to reduce the likelihood of personal data falling into the wrong hands, being lost, or being misused, to the lowest reasonable and practicable level and to mitigate the harm that would arise if a breach were to occur.

The policy applies to all employees (including agency, casual and temporary staff), volunteers (including trustees), contractors (whether on or off site) and others with access to any data (including students, trainees and interns). The term 'staff' may be used in this policy to refer to all or any of these.

Underlying principles
The Charity takes a risk-based approach. Security measures are appropriate to the risk posed by a potential breach.

Staff are authorised to access only the information that they need to know in order to carry out their duties. The Charity trusts its staff to treat confidential information appropriately but still recognises the need to limit their access in order to reduce risk further. Security measures aim to ensure that any particular person sees only the information that they are authorised to access and use.

The Charity recognises that effective security is not just a matter of technical measures. Therefore all staff are given appropriate guidance and training on security before being given access to confidential information and at appropriate intervals thereafter.

Steps to prevent unauthorised access to its premises and to the data it holds, and to prevent loss or damage to data

Particular care over data that leaves its premises, either for use by its staff or in transmission to other organisations or people. Steps are taken to ensure that the data arrives at its intended destination but also to render it inaccessible should it be lost or stolen en route.

Roles and responsibilities
Trustees
The Board is responsible for ensuring that this policy is reviewed regularly and amended in accordance with changes in technology as well as in data protection legislation (including the GDPR) and other regulatory requirements, and for appointing the Data Protection Officer.

Data Protection Officer and other managers

The Data Protection Officer is the Chief Executive and is responsible for:

- ensuring that this policy is adhered to by all employees, volunteers and contractors,
- ensuring that contracts with Data Processors comply with the GDPR from 25 May 2018, and include the necessary security provisions, and
- handling information security incidents.

The Data Protection Officer may ask other Directors to assist in fulfilling their duties. In particular:

- Through the IT support officer, for controlling all IT network access and for managing the relationship with external IT providers.
- Authorisation to access the network/terminate access is the responsibility of the relevant ELT member or their nominated delegate.
- Senior managers are responsible for ensuring data security within their area of responsibility.

Deliberate breaches of security by employees or volunteers are treated as serious disciplinary matters, and may be reported to the police where appropriate.

Individuals

All staff are required to read this policy and other related policies as part of their induction. Access to the IT network will only be given following completion of the Acceptable Use Policy Form.

All staff are required to report any security breaches, possible breaches or 'near misses' to the Data Protection Officer at the earliest opportunity, whether they are responsible for the incident or not.

Premises and equipment

The Charity controls access to its premises. Visitors are escorted and supervised at all times and must wear a clearly visible visitor badge.

The main locations within the premises where confidential information is held receive additional levels of access control – generally locked storage. This includes the IT server room and paper storage of HR records.

Access to material taken off-site, including paper archives and electronic back-ups, is also controlled.

The Charity protects its equipment from theft, damage and compromise, and maintains it in effective working condition.

Equipment is only removed from sites with prior authorisation and, if it is being disposed of, steps are taken to remove or securely overwrite confidential information beforehand.

The Charity maintains a policy setting out the conditions under which staff are authorised to use their personal electronic devices and equipment to process data.

IT system management

The Head of Facilities and IT has overall responsibility for IT systems. These responsibilities include:

- Ensuring that users have access to appropriate, authorised operating procedures, which are kept up to date;

- Ensuring that system changes are controlled;
- Segregating duties, where practicable, to reduce the risk of unauthorised access or modification of systems or data;
- Managing and monitoring relationships with third party suppliers to ensure that they comply with security requirements;
- Setting acceptance criteria for new systems and upgrades;
- Ensuring that a robust and reliable back-up procedure is in place and fully operational;
- Maintaining adequate network security; and
- Maintaining controls to detect, prevent and recover from malicious code.

Testing and development is separated from live systems, wherever possible, to minimise the risk of compromise to live data.

Data in transit
The Charity selects the most appropriate means for transmission of data, based on practicality and risk. Where a more secure alternative is available it is used, unless the cost or inconvenience is unjustified. Fax transmission is regarded as insecure unless the recipient indicates otherwise.

Users are given guidance to ensure that:

- Data is transmitted only to authorised recipients.
- The level of security is agreed between the Charity and the recipient to be appropriate.
- The agreed security measures are effectively applied.

The Charity regards email as, in many cases, an appropriate means of transmitting personal data – including sensitive personal data – provided the data is protected through encryption within the email and/or within an attachment. Uploading data files to a secure site is also regarded as appropriate

When e-mails are sent to more than one person at the same time, the Charity ensures that e-mail addresses are not disclosed to other recipients unless the sender is certain that it is appropriate for the whole group to have each other's addresses.

Where data is held on portable electronic devices, including but not restricted to USB sticks, laptops, tablets, smartphones and cameras, the following principles apply:

- The use of the device must be authorised, either through a general policy or on a case by case basis.
- Data will only be placed on a portable device where no practical alternative exists.
- Staff are expected to take appropriate care to prevent the device being lost or stolen, whether it belongs to them or to the Charity.
- The device must be protected by a password or access code if this is available.
- The data on the device should be encrypted where this is possible and appropriate.
- Devices that have been attached to other systems while in transit must be scanned for malware before being connected back to Ambitious about Autism systems.

Access control
Access control is based on Authorisation and Authentication.

Relevant senior managers authorise employees and volunteers to have access to the systems and data they require, under a formal process.

Access to systems is via username and password. Usernames and passwords are allocated to individuals (with a small number of generic log-ons which give limited access for visitors and other casual users). Passwords are required to meet a defined level of strength.

Ambitious about Autism regards it as a disciplinary (and potentially criminal) offence to log on under false credentials or to provide another person with unauthorised log-on credentials.

Access credentials are revoked promptly when no longer required – for example when the member of staff or volunteer no longer works for the Charity.   With ELT agreement an account may be kept active for a defined period after a staff member has left so that access to emails, for example, remains possible. In this case the account password is changed.

Where possible, logging on to applications is authenticated by Active Directory, in order to avoid multiple user credential stores and to permit activity logging.

Authorised users outside the premises are able to access the IT system only through secure means.

Monitoring

The Charity reserves the right to monitor its IT systems for the purposes of:

- Preventing and detecting criminal activities
- Investigating unauthorised access and use of data
- Establishing compliance with regulatory standards and Ambitious about Autism policies
- Ensuring effective IT system operation

Any monitoring is proportionate to the assessed risk.

Personal use and personal devices

Personal use of systems is governed by an Acceptable Use Policy.

Where staff are authorised to work from home, the Charity reserves the right to determine which security measures are required and to carry out reasonable assessments to satisfy itself that these are in place.

Wherever possible, staff working from home or other remote locations are required to log into the central system remotely, and not to store or print confidential information locally.

Information security incidents

The Data Protection Officer is responsible for handling information security incidents.

These are investigated promptly, remedial action is taken, and lessons learned, following the principles set out in the Information Commissioner’s Guidance on data security breach management. In particular the Data Protection Officer will address:

1) **Containment and recovery**: investigating the breach and putting in place any relevant measures to prevent any further breach and/or recover losses and mitigate damage.
2) **Assessing the risks**: in particular the likelihood and potential extent of adverse consequences for individuals.
3) **Notification of the breach**: deciding whether to notify affected individuals and/or regulatory bodies (see below).
4) **Evaluation and response**: making recommendations to reduce the likelihood of a similar breach in future or to improve Ambitious about Autism’s response to security breaches.

The decision on whether to notify anyone about the breach (and advise them of steps they might take) is likely to depend on factors such as:

- legal, contractual or regulatory requirements;

- the benefit to individuals of informing them – for example if they can take mitigating action;
- the number of people affected;
- the vulnerability of the people affected; and
- the consequences of alarming people unnecessarily if the breach is not serious.

Other policies to be referred to:

- Confidentiality Policy
- Data Protection Policy
- Disciplinary Policy
- Acceptable Use of IT Policy and Procedure
- Use and storage of digital media
- Contracts of Employment
- Child Safeguarding and Protection Policy
- Adult Safeguarding Policy and Procedure
- External Communication Policy
- Recruitment Policy and Procedure

Top Ten

1. Take great care whenever you send confidential email to someone else, to ensure that you send it to the right person (or people) and with the right level of protection.

2. Do not share your username and password, or other access credentials, with anyone. If they need to see the data you manage, ask for guidance on a better way to do this.

3. Do not take documents containing confidential information out of Ambitious about Autism premises without a very good reason. Then take the minimum necessary, and take great care not to lose it.

4. Take responsibility for your visitors to Ambitious about Autism, and challenge anyone on the premises you are not sure of.

5. When sending information electronically, check that your file or document does not contain hidden information that it is not supposed to (e.g. in document properties or on worksheets that are not immediately displayed).

6. Do not work on Ambitious about Autism information from home unless you have been authorised to do so and had your security checked.

7. Never use your own personal cloud accounts (such as Dropbox, Google Drive, etc.) for holding, transmitting or working on Ambitious about Autism information.

8. Practice ‘clear desk, clear screen’ so that information is not left unattended where other people might see it.

9. Do not fax confidential information unless it really is the only alternative, and then make sure the recipient is standing by to receive it before sending.

10. Report any security breaches or ‘near misses’ you are aware of, whether or not you caused it.