##

##

**SECURITY BREACH PREVENTION POLICY**

|  |  |  |  |
| --- | --- | --- | --- |
| Date of last review: | **March 2018** | Review period: | **2 years** |
| Date of next review: | **March 2020** | Owner: | **AAT DFO** |
| Type of policy: | **Statutory/network** | LAB or Board approval: | **Board** |

## Security Breach Prevention Policy

1. **Statement of Intent**

The Aspirations Academies Trust is committed to maintaining the confidentiality of its information and ensuring that the details of the finances, operations and individuals within the Trust are only accessible by the appropriate individuals. It is therefore important to uphold high standards of security, take suitable precautions, and to have systems and procedures in place that support this.

The Trust recognises, however, that breaches in security can occur, particularly as the majority of information is stored online or on electronic devices which are increasingly vulnerable to cyber-attacks. This being the case, it is necessary to have a contingency plan containing procedures to minimise the potential negative impacts of any security breach, to alert the relevant authorities, and to take steps to help prevent a repeat occurrence.

For the purposes of this policy, the title of ‘data controller’ will be used in reference to the person(s) primarily responsible for the handling and protection of information and data within an individual academy.

1. **Legal framework**

This policy has due regard to statutory legislation and regulations including, but not limited to, the following:

* The Data Protection Act 1998
* The Computer Misuse Act 1990
* The General Data Protection Regulation (GDPR)

This policy has due regard to the Trust’s policies and procedures including, but not limited to, the following:

* E-Safety Policy
* Data Protection Policy
* Acceptable Use Policy
1. **Types of security breach and causes**

**Unauthorised use without damage to data** – involves unauthorised persons accessing data on the Trust system, e.g. ‘hackers’, who may read the data or copy it, but who do not actually damage the data in terms of altering or deleting it.

**Unauthorised removal of data** – involves an authorised person accessing data, who removes the data to pass it on to another person who is not authorised to view it, e.g. a staff member with authorised access who passes the data on to a friend without authorised access – this is also known as data theft. The data may be forwarded or deleted altogether.

**Damage to physical systems** – involves damage to the hardware in the Trust’s ICT system, which may result in data being inaccessible to the Trust and/or becoming accessible to unauthorised persons.

**Unauthorised damage to data** – involves an unauthorised person causing damage to data, either by altering or deleting it. Data may also be damaged by a virus attack, rather than a specific individual.

Breaches in security may be caused as a result of actions by individuals, which may be accidental, malicious or the result of negligence – these can include:

* Accidental breaches, e.g. as a result of insufficient training for staff, so they are unaware of the procedures to follow.
* Malicious breaches, e.g. as a result of a hacker wishing to cause damage to the Trust through accessing and altering, sharing or removing data.
* Negligence, e.g. as a result of an employee that is aware of Trust policies and procedures, but disregards these.

Breaches in security may also be caused as a result of system issues, which could involve incorrect installation, configuration problems or an operational error – these can include:

* Incorrect installation of anti-virus software and/or use of software which is not the most up-to-date version, meaning the Trust software is more vulnerable to a virus
* Incorrect firewall settings are applied, e.g. access to the Trust network, meaning individuals other than those required could access the system
* Confusion between backup copies of data, meaning the most recent data could be overwritten
1. **Roles** **and responsibilities**

The Principal, in conjunction with the Trust executive, is responsible for implementing effective strategies for the management of risks posed by internet use, and to keep its network services, data and users secure.

The data controller is responsible for the overall monitoring and management of data security.

The Principal is responsible for establishing a procedure for managing and logging incidents.

The Trust executive is responsible for holding regular meetings with the Principal and data controller to discuss the effectiveness of data security, and to review incident logs.

All members of staff and pupils are responsible for adhering to the processes outlined in this policy, alongside the Trust’s E-Safety Policy and Acceptable Use Policy.

1. **Secure configuration**

An inventory will be kept of all IT hardware and software currently in use at the Trust, including mobile phones and other personal devices provided by the Trust. This will be stored in the academy office and will be audited on a termly basis to ensure it is up-to-date.

Any changes to the IT hardware or software will be documented using the inventory, and will be authorised by the data controller before use.

All systems will be audited on a termly basis to ensure the software is up-to-date. Any new versions of software or new security patches will be added to systems, ensuring that they do not affect network security, and will be recorded on the inventory.

Any software that is out-of-date or reaches its ‘end of life’ will be removed from systems, i.e. when suppliers end their support for outdated products such that any security issues will not be rectified.

All hardware, software and operating systems will require passwords for individual users before use. Passwords will be changed on a termly basis to prevent access to facilities which could compromise network security.

The Trust believes that locking down hardware, such as through the use of strong passwords, is an effective way to prevent access to facilities by unauthorised users.

1. **Network security**

The Trust will employ firewalls in order to prevent unauthorised access to the systems.

The Trust’s firewall will be deployed as either a:

* Centralised deployment: the broadband service connects to a firewall that is located within a data centre or other major network location.
* Localised deployment: the broadband service connects to a firewall that is located on an appliance or system on the Trust premises, as either discrete technology or a component of another system.

For centralised deployments, as the Trust’s firewall is managed locally by a third party, the firewall management service will be thoroughly investigated by the data controller to ensure that:

* Any changes and updates that are logged by authorised users within the Trust are undertaken efficiently by the provider to maintain operational effectiveness.
* Patches and fixes are applied quickly to ensure that the network security is not compromised.

For localised deployments, as the Trust’s firewall is managed on the premises, it is the responsibility of the data controller to effectively manage the firewall. The data controller will ensure that:

* The firewall is checked weekly for any changes and/or updates, and that these are recorded using the inventory.
* Any changes and/or updates that are added to servers, including access to new services and applications, are checked to ensure that they do not compromise the overall network security.
* The firewall is checked weekly to ensure that a high level of security is maintained and there is effective protection from external threats.
* Any compromise of security through the firewall is recorded using an incident log and is reported to the Principal. The data controller will react to security threats to find new ways of managing the firewall.

For centralised deployments the Trust will consider installing additional firewalls on the servers in addition to the third-party service as a means of extra network protection. This decision will be made by the Principal, taking into account the level of security currently provided and any incidents that have occurred.

1. **Malware prevention**

The Trust understands that malware can be damaging for network security and may enter the network through a variety of means, such as email attachments, social media, malicious websites or removable media controls.

The data controller will ensure that all Trust devices have secure malware protection and undergo regular malware scans.

The data controller will update malware protection on a termly basis to ensure it is up-to-date and can react to changing threats.

Malware protection will also be updated in the event of any attacks to the Trust’s hardware and software.

Filtering of websites will ensure that access to websites with known malware is blocked immediately and reported to the data controller.

The Trust will use mail security technology, which will detect and block any malware that is transmitted by email. This will also detect any spam or other messages which are designed to exploit users.

The data controller will review the mail security technology on a termly basis to ensure it is kept up-to-date and effective.

1. **User privileges**

The Trust understands that controlling what users have access to is important for promoting network security. User privileges will be differentiated, i.e. pupils will have different access to data and the network than members of staff.

The Principal will clearly define what users have access to and will communicate this to the data controller, ensuring that a written record is kept.

The data controller will ensure that user accounts are set up to allow users access to the facilities required, in line with the Principal’s instructions, whilst minimising the potential for deliberate or accidental attacks on the network.

The data controller will ensure that websites are filtered on a weekly basis for inappropriate and malicious content. Any member of staff or pupil that has accessed inappropriate or malicious content will be recorded in accordance with the monitoring process in this policy.

All users will be required to change their passwords on a termly basis and must use upper and lowercase letters, as well as numbers, to ensure that passwords are strong. Users will also be required to change their password if they become known to other individuals.

Pupils are responsible for remembering their passwords; however, the data controller will have an up-to-date record of all usernames and passwords, and will be able to reset them if necessary.

Pupils in KS1 will not have individual logins, and class logins will be used instead. If it is appropriate for a pupil to have an individual login, the data controller will set up their individual user account, ensuring appropriate access and that their username and password is recorded.

The ‘master user’ password used by the data controller will be made available to the Principal, or any other nominated senior leader, and will be kept in the academy office.

A multi-user account will be created for visitors to the Trust, such as volunteers, and access will be filtered as per the Principal’s instructions. Usernames and passwords for this account will be changed on a termly basis, and will be provided as required.

Automated user provisioning systems will be employed in order to automatically delete inactive users or users who have left the Trust. The data controller will manage this provision to ensure that all users that should be deleted are, and that they do not have access to the system.

The data controller will review the system on a termly basis to ensure the system is working at the required level.

1. **Monitoring usage**

Monitoring user activity is important for the early detection of attacks and incidents, as well as inappropriate usage by pupils or staff.

The Trust will inform all pupils and staff that their usage will be monitored, in accordance with the Trust’s Acceptable Use Policy and E-Safety Policy.

If a user accesses inappropriate content or a threat is detected, an alert will be sent to the data controller. Alerts will also be sent for unauthorised and accidental usage.

Alerts will identify: the user, the activity that prompted the alert and the information or service the user was attempting to access.

The data controller will record any alerts using an incident log and will report this to the Principal. All incidents will be responded to in accordance with this policy, and as outlined in the E-Safety Policy.

All data gathered by monitoring usage will be kept in a filing cabinet in the academy office for easy access when required. This data may be used as a method of evidence for supporting a not yet discovered breach of network security. In addition, the data may be used to ensure the Trust is protected and all software is up-to-date.

1. **Removable media controls and home working**

The Trust understands that pupils and staff may need to access the Trust network from areas other than on the premises. Effective security management will be established to prevent access to, or leakage of, data, as well as any possible risk of malware.

The data controller will encrypt all Trust-owned devices for personal use, such as laptops, USB sticks and tablets, to ensure that they are password protected. If any portable devices are lost, this will prevent unauthorised access to personal data.

Pupils and staff are not permitted to use their personal devices where the Trust shall provide alternatives, such as work laptops, tablets and USB sticks, unless instructed otherwise by the Principal.

Staff who use Trust-owned laptops, tablets and other portable devices will use them for work purposes only, whether on or off Trust premises.

The data controller will use encryption to filter the use of websites on these devices, in order to prevent inappropriate use and external threats which may compromise network security when bringing the device back onto the premises.

The Trust uses tracking technology where possible to ensure that lost or stolen devices can be retrieved.

All data will be held on systems centrally in order to reduce the need for the creation of multiple copies, and/or the need to transfer data using removable media controls.

The Wi-Fi network at the Trust will be password protected and will only be given out as required. Staff and pupils are not permitted to use the Wi-Fi for their personal devices, such as mobile phones or tablets, unless instructed otherwise by the Principal.

A separate Wi-Fi network will be established for visitors at the Trust to limit their access to printers, shared storage areas and any other applications which are not necessary.

1. **Backing-up data**

The data controller performs a back-up of all electronic data held by the Trust on a weekly basis, and the date of the back-up is recorded using a log. Each back-up is retained for three months before being deleted.

The data controller performs an incremental back-up on a daily basis of any data that has changed since the previous back-up.

Where possible, back-ups are run overnight and are completed before the beginning of the next school day.

Upon completion of back-ups, data is stored on the Trust’s hardware which is password protected.

Only authorised personnel are able to access the Trust’s data.

1. **User training and awareness**

The data controller and Principal will arrange training for pupils and staff on a regular basis to ensure they are aware of how to use the network appropriately in accordance with the Acceptable Use Policy and E-Safety Policy.

Training for all staff members will be arranged by the data controller within two weeks following an attack or significant update.

Through training, all pupils and staff will be aware of who they should inform first in the event that they suspect a security breach, and who they should inform if they suspect someone else is using their passwords.

All staff will receive training as part of their induction programme, as well as any new pupils that join the Trust.

All users will be made aware of the disciplinary procedures for the misuse of the network leading to malicious attacks, in accordance with the process detailed in the E-Safety Policy.

1. **Security breach incidents**

Any individual that discovers a security data breach will report this immediately to the Principal and data controller.

When an incident is raised, the Principal will record the following information:

* Name of the individual who has raised the incident
* Description of the incident
* Description of any perceived impact
* Description and identification codes of any devices involved, e.g. Trust-owned laptop
* Location of the equipment involved
* Contact details for the individual who discovered the incident

The Trust’s data controller will take the lead in investigating the breach, and will be allocated the appropriate time and resources to conduct this.

The data controller, as quickly as reasonably possible, will ascertain the severity of the breach and determine if any personal data is involved or compromised.

The data controller will oversee a full investigation and produce a comprehensive report.

The cause of the breach, and whether or not it has been contained, will be identified – ensuring that the possibility of further loss/jeopardising of data is eliminated or restricted as much as possible.

If the data controller determines that the severity of the security breach is low, the incident will be managed in accordance with the following procedures:

* In the event of an internal breach, the incident is recorded using an incident log, and by identifying the user and the website or service they were trying to access.
* The Principal will issue disciplinary sanctions to the pupil or member of staff, in accordance with the processes outlined in the E-safety Policy.
* The data controller will work with the third-party provider to provide an appropriate response to the attack, including any in-house changes.

Any further action which could be taken to recover lost or damaged data will be identified – this includes the physical recovery of data, as well as the use of back-ups.

Where the security risk is high, the Trust will establish what steps need to be taken to prevent further data loss which will require support from various Trust departments and staff. This action will include:

* Informing relevant staff of their roles and responsibilities in areas of the containment process.
* Taking systems offline.
* Retrieving any lost, stolen or otherwise unaccounted for data.
* Restricting access to systems entirely or to a small group.
* Backing up all existing data and storing it in a safe location.
* Reviewing basic security, including:
* Changing passwords and login details on electronic equipment.
* Ensuring access to places where electronic or hard data is kept is monitored and requires authorisation.

Where appropriate, e.g. if offences have been committed under the Computer Misuse Act 1990, the data controller will inform the police of the security breach.

The data controller will test all systems to ensure they are functioning normally, and the incident will only be deemed ‘resolved’ when it has been assured that the Trust’s systems are safe to use.

1. **Assessment of risks**

The following questions will be considered by the data controller in order to fully and effectively assess the risks that the security breach has brought, and to help take the next appropriate steps. All relevant questions will be clearly and fully answered in the data controller’s report and records:

* What type and how much data is involved?
* How sensitive is the data? Sensitive data is defined in the Data Protection Act 1998; some data is sensitive because of its very personal nature (e.g. health records) while other data types are sensitive because of what might happen if it is misused (e.g. bank account details).
* Is it possible to identify what has happened to the data – has it been lost, stolen, deleted or tampered with?
* If the data has been lost or stolen, were there any protective measures in place to prevent this, such as data and device encryption?
* If the data has been compromised, have there been effective measures in place that have mitigated the impact of this, such as the creation of back-up tapes and spare copies?
* Has individuals’ personal data been compromised – how many individuals are affected?
* Who are these individuals – are they pupils, staff, governors, volunteers, stakeholders, suppliers?
* Could their information be misused or manipulated in any way?
* Could harm come to individuals? This could include risks to the following:
* Physical safety
* Emotional wellbeing
* Reputation
* Finances
* Identity
* Private affairs becoming public
* Are there further implications beyond the risks to individuals? Is there a risk of loss of public confidence/damage to the Trust’s reputation, or risk to the Trust’s operations?
* Who could help or advise the Trust on the breach? Could external partners, authorities, or others provide effective support?

In the event that the data controller, or other persons involved in assessing the risks to the Trust, are not confident in the risk assessment, they will seek advice from the Information Commissioner’s Office (ICO).

1. **Consideration of further notification**

The Trust will consider whether there are any legal, contractual or regulatory requirements to notify individuals or organisations that may be affected or who will have an interest in security.

The Trust will decide whether notification will help the Trust meet its security obligations under the [seventh data protection principle](https://ico.org.uk/for-organisations/guide-to-data-protection/principle-7-security/).

The Trust will assess whether notification could help the individual(s) affected, and whether individuals could act on the information provided to mitigate risks, e.g. by cancelling a credit card or changing a password.

If a large number of people are affected, or there are very serious consequences, the ICO will be informed.

The Trust will consider who to notify, what to tell them and how they will communicate the message, which may include:

* A description of how and when the breach occurred and what data was involved. Details of what has already been done to respond to the risks posed by the breach will be included.
* Specific and clear advice on the steps they can take to protect themselves, and what the Trust is willing to do to help them.
* A way in which they can contact the academy for further information or to ask questions about what has occurred.

The Trust will consult the ICO for guidance on when and how to notify them about breaches.

The Trust will consider, as necessary, the need to notify any third parties – police, insurers, professional bodies, funders, trade unions, website/system owners, banks/credit card companies – who can assist in helping or mitigating the impact on individuals.

**Under the GDPR, the following steps will be taken if a breach of personal data occurs:**

The Trust will notify the ICO within 72 hours of a breach where it is likely to result in a risk to the rights and freedoms of individuals.

Where a breach is likely to result in significant risk to the rights and freedoms of individuals, the Trust will notify those concerned directly with the breach.

Where the breach compromises personal information, the notification will contain:

* The nature of the personal data breach including, where possible:
* The type(s), e.g. staff, pupils or governors, and approximate number of individuals concerned.
* The type(s) and approximate number of personal data records concerned.
* The name and contact details of the data controller or other person(s) responsible for handling the Trust’s information.
* A description of the likely consequences of the personal data breach.
* A description of the measures taken, or proposed, to deal with and contain the breach and, where appropriate, of the measures taken to mitigate any possible adverse effects.
1. **Evaluation and response**

The data controller will establish the root of the breach, and where any present or future risks lie.

The data controller will consider the data and contexts involved.

The data controller and Principal will identify any weak points in existing security measures and procedures.

The data controller and Principal will identify any weak points in levels of security awareness and training.

The data controller will report on findings and, with the approval of the Trust executive team, implement the recommendations of the report after analysis and discussion.

# Timeline of Incident Management

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Date** | **Time** | **Activity** | **Decision** | **Name/position** | **Date** |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |