Aspire
Educational Trust

Data and E-Security Breach Prevention and Management Plan

Contents:

Appendix

Statement of intent

The Aspire Educational Trust is committed to maintaining the confidentiality of its information and ensuring that the details of the finances, operations and individuals within the trust and its schools 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 Aspire Educational Trust recognises, however, that breaches in security can occur, particularly as most 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 a procedure 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.

1. Legal framework

1.1. This policy has due regard to statutory legislation and advisory guidance including, but not limited to, the following:

- The Computer Misuse Act 1990
- The General Data Protection Regulation (GDPR)
- National Cyber Security Centre (2018) ‘Cyber Security: Small Business Guide’

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

- E-safety Policy
- Data Protection Policy
- Acceptable Use Policy

2. Types of security breach and causes

2.1. **Unauthorised use without damage to data –** involves unauthorised persons accessing data on the school 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.

2.2. **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.

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

2.4. **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.

2.5. 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 school through accessing and altering, sharing or removing data.

- Negligence, e.g. as a result of an employee that is aware of school policies and procedures, but disregards these.

2.6. 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 school software is more vulnerable to a virus
- Incorrect firewall settings are applied, e.g. access to the school 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

3. Roles and responsibilities

3.1. The data protection officer (DPO) is responsible for:

- The overall monitoring and management of data security.
- Deciding which strategies are required for managing the risks posed by internet use, and for keeping the trust and its schools' network services, data and users safe, in conjunction with the e-safety leads and principals
- Leading on the trust's response to incidents of data security breaches.
- Assessing the risks to the trust and its schools in the event of a data security breach.
- Producing a comprehensive report following a full investigation of a data security breach.
- Determining which organisations and individuals need to be notified following a data security breach, and ensuring they are notified.
- Working with the e-safety lead and principal after a data security breach to determine where weaknesses lie and improve security measures.
- Organising training for staff members on data security and preventing breaches.
- Monitoring the effectiveness of this policy and communicating any changes to the trust and its staff members.

3.2. Each academy's e-safety lead working with the contracted IT technical support is responsible for:

- Maintaining an inventory of all ICT hardware and software currently in use at the school.

- Ensuring any software that is out-of-date is removed from the school premises.
- Implementing effective firewalls to enhance network security and ensuring that these are monitored regularly.
- Ensuring all school-owned devices have secure malware protection and that devices are regularly updated.
- Installing, monitoring and reviewing filtering systems for the school's network.
- Setting up user privileges in line with recommendations from the principal.
- Maintaining an up-to-date inventory of all usernames and passwords.
- Removing any inactive users from the school's system, ensuring that this is always up-to-date.
- Recording any alerts for access to inappropriate content and notifying the principal.
- Ensuring there is back-up of all electronic data held by the school, ensuring detailed records of findings are kept.
- Organising training for staff members on network security.

3.3. The principal is responsible for:

- Ensuring all staff members and pupils are aware of their responsibilities in relation to this policy.
- Defining users' access rights for both staff and pupils, communicating these to the e-safety lead.
- Responding to alerts for access to inappropriate content in line with the E-safety Policy.
- Organising training for staff members in conjunction with the e-safety lead and DPO.

4. Secure configuration

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

4.2. Any changes to the ICT hardware or software will be documented on the School Asset Register and will be authorised by the e-safety lead before use.

4.3. All systems will be audited regularly by the e-safety lead with support from IT technical support 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 in the inventory.

4.4. 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.

4.5. All hardware, software and operating systems will require passwords from individual users before use.

4.6. The trust and its schools will act on guidance from accredited organisations such as the National Cyber Security Centre to continuously develop and improve their cyber security.

5. Network security

5.1. The trust and its schools will employ firewalls in order to prevent unauthorised access to the systems.

5.2. How the trust and its schools deploy firewalls is a local decision and may be a centralised or localised deployment as detailed below:

- 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 school premises, as either discrete technology or a component of another system.

5.3. Schools where the firewall is managed locally by a third party, the firewall management service will be thoroughly investigated by the e-safety lead and principal to ensure that:

- Any changes and updates that are logged by authorised users within the school 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.

5.4. Schools where the firewall is managed on the premises, it is the responsibility of the e-safety lead and principal to effectively manage the firewall. They 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 DPO. The e-safety lead will react to security threats to find new ways of managing the firewall.

5.5. Schools where there is centralised deployments 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 e-safety lead and the principal, taking into account the level of security currently provided and any incidents that have occurred.

6. Malware prevention

6.1. The trust and its schools understand 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.

6.2. Each school will ensure that all school devices have secure malware protection and undergo regular malware scans in line with specific requirements.

6.3. Each school will update malware protection regularly to ensure it is up-to-date and can react to changing threats.

6.4. Malware protection will also be updated in the event of any attacks to a school's hardware and software.

6.5. Filtering of websites, as detailed in section 7 of this policy, will ensure that access to websites with known malware are blocked immediately and reported to the e-safety lead.

6.6. The trust and its schools 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.

6.7. The e-safety lead with IT technical support will review the mail security technology regularly to ensure it is kept up-to-date and effective.

6.8. Staff members are only permitted to download apps on any school-owned device from manufacturer-approved stores and with prior approval from the e-safety lead.

6.9. Where apps are installed, the e-safety lead with IT technician support will keep up-to-date with any updates, ensuring updates are installed without delay.

7. User privileges

7.1. The trust and its schools understand 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.

7.2. The principal will clearly define what users have access to and will communicate this to the e-safety lead and IT technical support staff.

7.3. The e-safety lead and IT technical support staff 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.

7.4. The e-safety lead and IT technical support staff will ensure that websites are filtered on a regularly 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 section 13 of this policy.

7.5. All users will be required to use strong passwords. Advice will be given on the best passwords to use.

7.6. Users will also be required to change their password if they become known to other individuals.

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

7.8. Any record of usernames and passwords will be stored securely.

7.9. Each academy will decide whether children will have class or individual logins based on their knowledge of the pupils and levels of risk. For monitoring purposes it is advised that in KS2 pupils may require individual logins.

7.10. Any 'master user' password used by the e-safety lead or IT technical support staff will be made available to the principal, DPO and any other nominated senior leader, and will be kept in the school office.

7.11. Two factor authentication logins will be considered for some accounts based on the level of security and risk identified.

7.12. The master user account is used as the 'administrator' which allows designated users to make changes that will affect other users' accounts in the school, such as changing security settings, monitoring use, and installing software and hardware.

7.13. A multi-user account will be created for visitors to the school, such as volunteers and supply teachers, and access will be filtered as per the principal's instructions. Usernames and passwords for this account will be changed regularly and will be provided as required.

7.14. The e-safety lead will ensure that all users who are no longer authorised to access the system are promptly deleted, and that they do not have access to the system.

7.15. The e-safety lead will review the system regularly to ensure the system is working at the required level.

8. Monitoring usage

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

8.2. Each school will risk assess the level of monitoring required and may choose to either use physical or active technology monitoring.

8.3. Each school will inform all pupils and staff that their usage will be monitored, in accordance with the school's Acceptable Use Policy and E-safety Policy.

8.4. If a user accesses inappropriate content or a threat is detected, an alert will be sent to the e-safety lead. Alerts will also be sent for unauthorised and accidental usage.

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

8.6. The e-safety lead will record any alerts using an incident log and will report this to the principal and in some circumstances the Designated Safeguarding Lead. All incidents will be responded to in accordance with section 13 of this policy, and as outlined in the school's E-safety Policy.

8.7. All data gathered by monitoring usage will be filed 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 school is protected and all software is up-to-date.

9. Removable media controls and home working

9.1. The trust understands that pupils and staff may need to access their 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.

9.2. School-owned devices are password-protected to protect the information on the device in case of theft.

9.3. Where possible, the trust and its schools enable electronic devices to allow the remote blocking or deletion of data in case of theft.

9.4. Before distributing any school-owned devices, the school will ensure that manufacturers' default passwords have been changed.

9.5. Pupils and staff are not permitted to use their personal devices where the school provides alternatives, such as work laptops and tablets unless instructed otherwise by the principal.

9.6. If pupils and staff are instructed that they are able to use their personal devices, they will ensure that they have an appropriate level of security and firewall to prevent any compromise of the school's network security. This will be checked by the school.

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

9.8. Trust computers and portable devices such as laptops and tablets will be used whenever possible. Staff, governors and trustees will not use their personal devices for trust purposes involving the storing of personal data. When working on personal data away from trust sites staff and governors will adhere to the same data security procedures expected when working on trust premises.

9.9. Staff members will avoid connecting to unknown Wi-Fi hotspots, such as in coffee shops, when using any laptops, tablets or other devices.

9.10. Memory sticks will not be used to hold personal information unless they are password-protected and fully encrypted. Personal memory sticks will not be used. The trust and its schools will issue staff with encrypted memory sticks and log who has possession of these memory sticks. Issued memory sticks must be returned when employment ceases.

9.11. The trust and its schools 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.

9.12. Where possible 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.

9.13. The Wi-Fi network at each school 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.

10. Backing-up data

10.1. The trust and its schools perform a remote back-up of all electronic data held by the school on their servers on a daily basis.

10.2. The trust and its schools may also choose to use cloud based computing which means data is physically separate from their location. The trust and its schools will make checks of their providers built-in security practices.

10.3. Staff are given advice, training and support to securely back-up data stored on their portable devices. Staff are responsible for ensuring they back-up their own data regularly.

10.4. Only authorised personnel are able to access the school's data.

11. Avoiding phishing attacks

11.1. The trust and its schools will configure all staff accounts using the principle of 'least privilege' – staff members are only provided with as much rights as are required to perform their jobs.

11.2. Designated individuals who have access to the master user account will avoid browsing the web or checking emails whilst using this account.

11.3. Where possible two-factor authentication is used on any important accounts.

11.4. In accordance with section 12 of this policy, the trust and its schools will organise regular training for staff members – this will cover identifying irregular emails in order to help staff members spot requests that are out of the ordinary, such as receiving an invoice for a service not used, and who to contact if they notice anything unusual.

11.5. Staff will use the following warning signs when considering whether an email may be unusual:

- Is the email from overseas?
- Is the spelling, grammar and punctuation poor?
- Is the design and quality what you would expect from a large organisation?
- Is the email addressed to a 'valued customer', 'friend' or 'colleague'?
- Does the email contain a veiled threat that asks the staff member to act urgently?
- Is the email from a senior member of the school asking for a payment?
- Does the email sound too good to be true? It is unlikely someone will want to give another individual money or access to another service for free.

11.6. The trust and its schools will ensure that email filtering systems, applied in accordance with section 6 of this policy, are neither too strict or lenient; filtering that is too strict may lead to legitimate emails becoming lost, and too lenient filters may mean that emails that are spam or junk are not sent to the relevant folder.

11.7. To prevent hackers having access to unnecessary public information, the DPO will ensure the school's social media accounts and websites are reviewed on an annual basis, making sure that only necessary information is shared.

11.8. Principals will ensure parents, pupils, staff and other members of the school community are aware of acceptable use of social media and the information they share about the school and themselves, in accordance with the trust and its schools Acceptable Use Policy.

12. User training and awareness

12.1. The trust and its schools 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.

12.2. Principals will arrange awareness training for staff on an annual basis on maintaining data security, preventing data breaches, and how to respond in the event of a data breach.

12.3. Schools will include protecting data, preventing breaches and how to respond in the event of a data breach within the e-safety curriculum map.

12.4. If required, training for relevant staff members will be arranged by the trust and its schools within two weeks following an attack, breach or significant update.

12.5. 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.

12.6. All staff will receive training as part of their induction programme, as well as any new pupils who join the school.

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

13. Security breach incidents

13.1. Any individual that discovers a security data breach will report this immediately to the principal and the DPO.

13.2. When an incident is raised, the DPO will record the following information on the AET data breach notification record:

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

13.3. The trust’s DPO will take the lead in investigating the breach and will be allocated the appropriate time and resources to conduct this.

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

13.5. The DPO will oversee a full investigation and produce a comprehensive report.

13.6. 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.

13.7. If the DPO 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.
- In the event of any external or internal breach, the DPO will record this using an incident log and respond appropriately, e.g. by updating the firewall, changing usernames and passwords, updating filtered websites or creating further back-ups of information.
- The data controller will work with any third-party provider to provide an appropriate response to the attack, including any in-house changes.

13.8. 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.

13.9. Where the security risk is high, the DPO will establish which steps need to be taken to prevent further data loss which will require support from the trust, its schools 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.

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

13.11. Where the school has been subject to online fraud, scams or extortion the DPO will also report this using the Action Fraud website.

13.12. The affected school 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 school's systems are safe to use.

14. Assessment of risks

14.1. The following questions will be considered by the DPO 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 DPO's report and records:

- What type and how much data is involved?
- How sensitive is the data? Sensitive data is defined in the GDPR; 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 school's reputation, or risk to the school's operations?
- Who could help or advise the school on the breach?

14.2. In the event that the DPO, or other persons involved in assessing the risks to the school, are not confident in the risk assessment, they will seek advice from the ICO.

15. Consideration of further notification

15.1. The DPO 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 (see 15.8 onwards for specific GDPR requirements about personal data).

15.2. The DPO 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.

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

15.4. The DPO 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 school is willing to do to help them.
- A way in which they can contact the school for further information or to ask questions about what has occurred.

15.5. The ICO will be consulted for guidance on when and how to notify them about breaches.

15.6. The DPO 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.

15.7. The DPO 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.

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

15.9. 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 DPO or other person(s) responsible for handling the school’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.

16. Evaluation and response

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

16.2. The DPO will consider the data and contexts involved.

16.3. The DPO and principal will identify any weak points in existing security measures and procedures.

16.4. The DPO will work with the principal to improve security procedures wherever required.

16.5. The DPO and principal will identify any weak points in levels of security awareness and training.

16.6. The DPO will report on findings and, with the approval of the trust leadership team, implement the recommendations of the report after analysis and discussion.

17. Monitoring and review

17.1. This policy will be reviewed by the DPO and, on an annual basis. The next scheduled review date for this policy is Autumn 2020.

17.2. The DPO is responsible for monitoring the effectiveness of this policy, amending necessary procedures and communicating any changes to staff member