GDPR Security Breach Prevention and Management Plan

Policy Author	Principal Business Manager/CFO
Date Last Reviewed	September 2020
Trust Key Reader	MS
Approved by Trust Board	22.10.20
Review Date	September 2021

Statement of Intent

The Trust is committed to maintaining the confidentiality of its information and ensuring that the details of the finances, operations and individuals within the Trust/its Academies 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 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 the Trust/its Academies.

1. Legal Framework

1.1 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 Regulations (GDPR)

1.2 This policy has due regard to Academy 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 Academy's system either internally or cloud based data, 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, someone reading personal data left on a desk.

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 friends without authorised access – this is also known as data theft.

2.3 Damage to Physical Systems – involved damage to the hardware in the Academy's ICT system, which may result in data being inaccessible to the Academy 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, malware, ransomware or similar 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 Trust/Academy through accessing and altering, sharing or removing data
- Negligence, e.g. as a result of an employee that is aware of Trust/Academy 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 Trust/Academy software is more vulnerable to a virus
- Incorrect firewall settings are applied, e.g. access to the Trust/Academy network, meaning individuals other than those required could access the system
- Confusion between back-up copies of data, meaning the most recent data could be overwritten.

2.7 Breaches may also occur when hard copies of data is lost or compromised.

3. Roles and Responsibilities

3.1 The **Trust's Chief 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.

3.2 The **Trust's ICT Managers** are responsible for the overall monitoring and management of data security in the Trust alongside each Academy's Principal, who is supported by the Data Lead, in regard to for physical security.

3.3 The **Chief Executive** is responsible for establishing a procedure for managing and logging incidents.

3.4 The **Board of Trustees** is responsible for holding periodic meetings with the **Chief Executive.** The **Chief Executive** will periodically meet with each Principal and Data Lead, ICT Managers and DPO to discuss the effectiveness of data security, and to review incident logs from each Academy.

3.5 All members of staff and students are responsible for adhering to the processes outlined in this policy, alongside the **Trust's e-Safety Policy** and **Acceptable Use Policy**.

4. Secure Configuration

4.1 The ICT Managers will maintain an inventory of programmable and/or threat protection ICT hardware and software currently in use.

4.2 Any security related changes to the relevant IT hardware and software may only be undertaken by ICT technical support colleagues.

4.3 All relevant hardware and software will be kept updated by subsequent versions of software or new security patches.

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

4.5 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.

5. Network Security

5.1 The Trust will employ firewalls and other security means in order to prevent unauthorised access to the systems.

5.2 Firewalls be deployed as either:

- **Centralised deployment:** the chosen connectivity service links to a firewall that is located within a data centre or another major network location

OR

- **Localised deployment:** the chosen connectivity service links to a firewall that is located on an appliance or system on the Academy premises, as either discrete technology or a component of another system.

5.3 If the Academy's firewall is managed locally by a third party, the firewall management services will be thoroughly investigated by the Trust ICT Managers to ensure that:

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

6. Malware Prevention

6.1 Each Academy 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.

6.2 The **ICT Managers** will ensure that all Trust devices have secure malware protection and undergo regular malware scans.

6.3 The **ICT Managers** will update malware protection as necessary 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 the Trust'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 is blocked immediately and reported to the **Trust ICT team**.

6.6 Each Academy will use mail security technology, which will detect and apply all appropriate malware protection that is transmitted by email. This will also use appropriate means to detect any spam or other messages which are designed to exploit users.

6.7 The **ICT Managers** will review the mail security technology as necessary to ensure it is kept up-to-date and effective.

7. User Privileges

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

7.2 The **Principal** of each Academy will clearly define what users have access to and will communicate this to the ICT Managers.

7.3 The **ICT Managers** will oversee that user accounts are set up to allow users access to the facilities required, whilst minimising the potential for deliberate or accidental attacks on the network.

7.4 The **ICT Managers** will ensure that websites are appropriately filtered for inappropriate and malicious content. Any member of staff or student that has accessed inappropriate or malicious content will be recorded in accordance with the monitoring process in Section 8 of this policy.

7.5 All staff users shall change their passwords on a **termly** basis. These passwords must include 6 characters that have upper and lower case letters and a number/special character. Users will also be required to change their password if they become known to other individuals. Student password shall be changed annually and shall include 6 or more characters.

7.6 Students are responsible for remembering their passwords. The Academy's **ICT team** will be able to reset them if necessary.

7.7 The "Administrator" password used by the **ICT Team** will be made available to each **ICT Managers**, and the Chief Executive, if requested.

7.8 Visitors to the Academy, such as volunteers, will be given a guest password to use the system with access permissions to functionality on an 'as necessary' basis, in accordance with ICT policies and legal basis.

7.9 Systems and procedures will be employed in order to disable inactive users or users who have left the Academy/Trust. The **ICT Managers** will manage this provision to ensure that all users are deleted in accordance with the Trust's data retention and deletion policy are, and that they do not have access to the system.

7.10 The **ICT Managers** will periodically review hardware and systems to ensure the systems are working satisfactorily.

8. Monitoring Usage

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

8.2 Each Academy will inform their students and staff that their usage will be monitored, in accordance with the Trust's **Acceptable Use Policy** and **e-Safety Policy**.

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

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

8.5 The **ICT Team** will record any alerts using an incident log and will report this to each **Principal**. All incidents will be responded to in accordance with Section 12 of this policy, and as outlined in the **e-Safety Policy**.

8.6 All data gathered by monitoring usage will be kept centrally in each Academy 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 Academy is protected and all software is up-to-date.

9. Removable Media Controls and Home Working

9.1 Students and staff may need to access the Academy network outside school. Effective security management will be established to prevent access to, or leakage of, data as well as any possible risk of malware.

9.2 The ICT Managers will encrypt all Trust-owned devices for personal use, such as laptops, USB sticks (if specifically permitted for use by the Chief Executive), mobile phones and tablets, to ensure that they are password protected. If any portable devices are lost, this will prevent unauthorised access to personal data.

9.3 Students and staff are not permitted to use their own devices unless authorised by the Academy Principal and in accordance with other LEAP Policies.

9.4 If students 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 Academy's network security. This will be checked by the **ICT Team** in accordance with Trust policies.

9.5 When using laptops, tablets and other portable devices, their **Principal** will agree the limitations for access to the network with the ICT managers, as described in Section 5 of this policy.

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

9.8 Each Academy shall follow Trust financial procedures regarding the recording and tracking of inventory/assets.

9.9 The Trust's server, connectivity infrastructure, implementation of O365 and connectivity provides to avoid the use of removable media.

9.10 The wi-fi network at each Academy will be password protected and will only be given out as required. Staff and students are permitted to use the wi-fi for their personal devices by connecting using the Academy BYOD guidance/ID system. When doing so, you agree to follow the **Acceptable Use Policy and Bring Your Own Device Policy**.

9.11 Guest accounts are created when visitors need access. Such accounts limit access to printers, shared storage areas and any other applications which are not necessary.

10. Backing-Up Data

10.1 The ICT Managers arrange for the back-up of all electronic data held in Academies, the nature and frequency of back-up must be consistent with an assessment of risk.

10.2 Upon completion of back-ups, data is stored on the Academy's hardware which is password protected.

10.3 Only authorised personnel are able to access the Academy's data.

11. User Training and Awareness

11.1 Each Academy's **Principal** will arrange training for students and staff to ensure they are aware of how to use the network appropriately in accordance with the **Acceptable Use Policy** and **e-Safety Policy**.

11.2 Appropriate refreshed and re-active update training will be facilitated by the Academy Principal as necessary.

11.3 Through training, all students 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.

11.4 All staff and students will be made aware of the **Acceptable Use Policy** when they join the Trust.

11.5 All users will be made aware of the disciplinary procedures for the misuse of the network leading to malicious attacks (see **e-Safety Policy** and **Behaviour Policy**).

12. Security Breach Incidents

12.1 Any individual that discovers a security data breach will report this immediately to their **Principal** and **ICT Mangers (electronic systems) or Operations Lead, who will inform the DPO**.

12.2 When an incident is raised, the **Principal** will record the following information and share this with the ICT Managers/Operations Lead:

- 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, eg Trust-owned laptop
- Location of the equipment involved
- Contact details for the individual who discovered the incident

12.3 The ICT Managers/Operations Lead will take the lead in investigating the breach and will be allocated the appropriate time and resources to conduct this.

12.4 The **ICT Managers/Operations Lead** will, forthwith, ascertain the severity of the breach and determine if any personal data is involved or compromised.

12.5 The **ICT Managers/Operations Lead** will oversee a full investigation and produce a comprehensive report.

12.6 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.

12.7 If the **ICT Managers/Operations Lead** determined 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 internet 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 student or member of staff, in accordance with the processes outlined in the **e-Safety Policy/Behaviour Policy**
- In the event of any external or internal breach, the **ICT Managers/Operations Lead** 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 **ICT Managers/Operations Lead** will provide an appropriate response.
- Keep the DPO informed

12.8 Any further action which could be taken to recover lost or damaged data will be identified – this includes the physical recovery of data/personal information.

12.9 Where the security risk is deemed high by the ICT Managers**/**Operations Lead, they/she/he will advise the Chief Executive what steps need to be taken to prevent further data loss. This action may 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.
- Keep the DPO informed

12.10 Where appropriate, e.g. if offences have been committed under the **Computer Misuse Act 1990**, the ICT Managers/Operations Lead will inform the Chief Executive and DPO. The Chief Executive will arrange to notify the police of the security breach.

12.11 The **ICT Managers** will test all electronic systems to ensure they are functioning normally, and the incident will only be deemed "resolved" when it has been assured that the Trust/Academy systems are safe to use.

13. Assessment of Risks

13.1 The following questions will be considered by the ICT Managers/Operations Lead 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 their 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 students, staff, Members, Trustees, 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 pubic
- 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 Academy's operations?
- Who could help or advise the Trust/Academy on the breach? Could the Local Authority, external partners, authorities, or others provide effective support?

13.2 In the event that the ICT Managers/Operations Lead, or other person(s) involved in assessing the risks to the Trust/Academy, are not confident in the risk assessment, they will seek advice from the DPO).

14. Consideration of Further Notification

14.1 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 (see paragraphs 14.8 onwards for specific GDPR requirements about personal data).

14.2 The ICT Managers/Operations Lead 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.

14.3 The ICO will be informed by the DPO where it is required under the GDPR.

14.4 The DPO will advise 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 Academy 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.

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

14.6 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:

14.7 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.

14.8 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.

14.9 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, students, Members, Trustees, 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 Academy'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.

15. Evaluation and Response

15.1 The ICT Managers/Operations Lead will establish the root of the breach and where any present or future risks lie.

15.2 The ICT Managers/Operations Lead will consider the data and contexts involved.

15.3 The ICT Managers/Operations Lead and **Principal** will identify any weak points in existing security measures and procedures.

15.4 The ICT Managers/Operations Lead and **Principal** will identify any weak points in levels of security awareness and training.

15.5 The ICT Managers/Operations Lead will report on findings and, with the approval of the Academy's Senior Leadership Team, implement the recommendations of the report after analysis and discussion.

16. Monitoring and Review

16.1 This policy will be reviewed by the Chief Executive, in conjunction with the **ICT Managers, Operations Lead and DPO**, on an annual basis.

16.2 The ICT Managers/Operations Lead is responsible for monitoring the effectiveness of the policy, amending necessary procedures and communicating any change to staff members.

Timeline of Incident Management

Date	Time	Activity	Decision	Name/position	Date