DATA SECURITY BREACH MANAGEMENT POLICY

Date Approved by Board:	3 July 2018
Date of Review:	July 2020
Responsible Department:	Information Services
Policy Applies to:	Wellspring Trust and all Academies within the Trust

The Equality Act 2010 requires public bodies, in carrying out their functions, to have due regard to the need to:

- *eliminate discrimination and other conduct that is prohibited by the Act*
- *advance equality of opportunity between people who share a protected characteristic and people who do not share it*
- *foster good relations across all characteristics - between people who share a protected characteristic and people who do not share it.*

In the development of this policy due regard has been given to achieving these objectives.

Executive Summary

Wellspring Academy Trust is committed to maintaining the confidentiality of its information and ensuring that details of the finances, operations and individuals within The Trust are only accessible by the appropriate individuals.

This policy outlines how The Trust aims to minimise the occurrence of data security breaches and the response should a breach occur.

Data breaches can take many forms (see Section 3) including: unauthorised use without damage to data, unauthorised removal of data, damage to physical systems, damage to data, malicious/accidental/negligence acts by individuals and system issues such as incorrect installation/incorrect firewall settings/back up errors.

All members of staff and pupils are responsible for adhering to the processes outlined in this policy (see Section 4) and other related policies.

IT Service providers will need to ensure that technical and procedural measures are in place. Where this is managed by a third party provider this should be documented in service level agreements or contracts in order for The Trust to demonstrate compliance. This policy recommends measures that can be taken, however it is for Information Owners and their respective IT service providers to ensure compliance (see Sections 5 to 10).

Systems for backing-up of all electronic data held must be in place (see Section 11). Where this is managed by a third party provider this should be documented in service level agreements or contracts.

Staff training and development is essential to reduce the likelihood of a data breach occurring (see Section 12). All staff have a responsibility to safeguard data and report potential breach incidents.

Any individual that discovers a security data breach will report this immediately to the Data Protection Officer (DPO) via privacy@wellspringacademies.org.uk and the local Data Protection Lead (DPL) in order that an investigation and assessment can be undertaken (see Sections 13-15). Should an incident be deemed reportable to the ICO this must be done within 72 hours of the breach been identified.

When an incident is raised, the Information Owner 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. school-owned laptop
- Location of the equipment involved
- Contact details for the individual who discovered the incident.

An evaluation of the breach management process (see Section 16) will take place following a breach occurring. Any areas for system improvement or training and development needs will be identified and a record maintained for audit purposes. A periodic evaluation of data security will form part of the Wellspring Assurance Framework review cycle.

Contents

1. Statement of Intent

1.1. Wellspring Academy Trust and its Academies (The Trust) is committed to maintaining the confidentiality of its information and ensuring that 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.

1.2. 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.

1.3. For the purposes of this policy,

1.3.1. The Trust appointed Data Protection Officer (DPO) will provide information, advice and guidance to the Trust and its identified Information Owners (IO) and Data Protection Leads (DPL).

1.3.2. The Information Owner possess overall responsibility for information and data within the Trust's Academies or Business Units. Typically, this will be the most senior person within an Academy (e.g. Executive Principal) or Business Unit (e.g. Chief Officer).

1.3.3. The Data Protection Leads (DPL) are the identified data controllers and will be used in reference to the identified person(s) who is responsible for handling and protection of information and data within their Academy or Business Unit. In addition, they will provide operational support capacity for the Information Owner. They will also establish systems and processes for data protection including audit and compliance.

2. Legal Framework

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

- The Computer Misuse Act 1990
- The General Data Protection Regulation 2018

2.2. This policy has due regard to other Trust policies and procedures including, but not limited to, the following:

- Data Protection Policy
- IT Acceptable Use Policy

3. Types of security breaches and causes

3.1. *Unauthorised use without damage to data* – involves unauthorised persons accessing data on Trust systems, 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.

3.2. *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.

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

3.4. *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.

3.5. *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 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.

3.6. *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:

3.6.1. Incorrect installation of anti-virus software and/or use of software which is not the most up-to-date version, meaning the software is more vulnerable to a virus

3.6.2. Incorrect firewall settings are applied, e.g. access to the network, meaning individuals other than those required could access the system
3.6.3. Confusion between backup copies of data, meaning the most recent data could be overwritten.

4. Roles and responsibilities

4.1. The Information Owner 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.

4.2. The Information Owner is responsible for the overall monitoring and management of data security.

4.3. The Information Owner is responsible for establishing a procedure for managing and logging incidents.

4.4. The Governing Body is responsible for holding regular meetings with the Information Owner to discuss the effectiveness of data security, and to review incident logs. This will take place via the Wellspring Assurance Framework meetings and will be further supported by the DPO.

4.5. All members of staff and pupils are responsible for adhering to the processes outlined in this policy and others related policies (e.g. Data Protection Policy).

5. Security Configuration

5.1. An inventory will be kept of all IT hardware and software currently in use, including mobile phones and other personal devices that may be provided. This will be stored and will be audited on a periodic basis to ensure it is up-to-date.

5.2. Any changes to the IT hardware or software will be documented using the inventory and will be authorised by the Information Owner before use.

5.3. All systems will be audited on a periodic 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.

5.4. 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.

5.5. All hardware, software and operating systems will require passwords for individual users before use. Passwords are to be changed periodically in line with The Trust's Password Policy to prevent access to facilities that could compromise network security.

5.6. 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.

6. Network Security

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

6.2. The Trust's firewall will be deployed as a:

- **[Centralised deployment *IT Managed Service Provider]**: the broadband service connects to a firewall that is located within a data centre or other major network location.

- **[Localised deployment *In house IT Service Provider]:** the broadband service connects to a firewall that is located on an appliance or system on premise, as either discrete technology or a component of another system.

6.3. [Centralised deployments only *IT Managed Service Provider] As the firewall is managed locally by a third party, the firewall management service will be thoroughly investigated by the Information Owner to ensure that:

6.3.1 Any changes and updates that are logged by authorised users are undertaken efficiently by the provider to maintain operational effectiveness.

6.3.2 Patches and fixes are applied quickly to ensure that the network security is not compromised.

6.4 **[Localised deployments only *In house IT Service Provider]** As the firewall is managed on the premises, it is the responsibility of the data controller to effectively manage the firewall. The Information Owner will ensure that:

6.4.1 The firewall is checked weekly for any changes and/or updates, and that these are recorded using the inventory.

6.4.2 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.

6.4.3 The firewall is checked weekly to ensure that a high level of security is maintained and there is effective protection from external threats.

6.4.4 Any compromise of security through the firewall is recorded using an incident log and is reported to the Information Owner. The Information Owner will react to security threats to find new ways of managing the firewall.

6.5 **[Centralised deployments only *IT Managed Service Provider]** The Information Owner or Trust may 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 Information Owner, taking into account the level of security currently provided and any incidents that have occurred.

7 Malware Prevention

7.1 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.

7.2 The IT Service Provider will ensure that all devices have secure malware protection and undergo regular malware scans.

7.3 The IT Service Provider will update malware protection on a periodic basis to ensure it is up-to-date and can react to changing threats.

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

7.5 Filtering of websites will ensure that access to websites with known malware is blocked immediately and reported to the IT Service Provider.

7.6 Mail security technology will be used, 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.

7.7 The IT Service Provider will review the mail security technology on a periodic basis to ensure it is kept up-to-date and effective.

8 User Privileges

8.1 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.

8.2 The Information Owner will clearly define what users have access to and will communicate this to the IT Service Provider, ensuring that a written record is kept.

8.3 The IT Service Provider will ensure that user accounts are set up to allow users access to the facilities required, in line with the Information Owners instructions, whilst minimising the potential for deliberate or accidental attacks on the network.

8.4 The IT Service Provider will ensure that websites are filtered on a periodic 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 Section 13 of this policy.

8.5 All users will be required to change their passwords on a periodic 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.

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

8.7 [Primary schools only] Pupils in KS1 may not have individual logins and class logins can be used instead. If it is appropriate for a pupil to have an individual login, the Information Owner will set up their individual user account, ensuring appropriate access and that their username and password is recorded.

8.8 The 'master user' password used by the data controller will be made available to the Information Owner.

8.9 A multi-user account (Guest) will be created for visitors and access will be filtered as per the Information Owner's instructions. Usernames and passwords for this account will be changed on a periodic basis and will be provided as required.

8.10 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.

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

9 Monitoring Use

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

9.2 The Trust will inform all pupils and staff that their usage will be monitored, in accordance with the IT Acceptable Use Policy.

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

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

9.5 The IT Service Provider will record any alerts using an incident log and will report this to the Information Owner. All incidents will be responded to in accordance with this policy.

9.6 All data gathered by monitoring usage will be stored digitally 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 that the entity is protected and all software is up-to-date.

10 Removable Media Controls and Home Working

10.1 The Trust understands that pupils and staff may need to access the 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.

10.2 The IT Service provider will encrypt all Trust-owned devices for personal use, such as laptops, USB sticks, 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.

10.3 Pupils and staff should not use their personal devices where the Trust shall provide alternatives, such as work laptops, tablets and USB sticks, unless instructed otherwise by the Information Owner.

10.4 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 network security. This will be approved by the Information Owner.

10.5 When using laptops, tablets and other portable devices the Information Owner will determine the limitations for access to the network, as described in this policy.

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

10.7 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.

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

10.9 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.

10.10 The Wi-Fi network 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 Information Owner.

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

11 Backing Up Data

11.1 The Information Owner should ensure systems for a back-up of all electronic data held, on a periodic basis, and the date of the back-up is recorded using a log. Each back-up is retained before being deleted.

11.2 The Information Owner performs an incremental back-up on a periodic basis of any data that has changed since the previous back-up. The Information Owner will record the date of any incremental back-up, alongside a list of the files that have been included in the back-up.

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

11.4 Upon completion of back-ups, data is stored on hardware which is password protected.

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

12 User Training and Awareness

12.1 The Information Owner will arrange training for pupils and staff on a periodic basis to ensure they are aware of how to use the network appropriately in accordance with the IT Acceptable Use Policy.

12.2 Training for all staff members will be arranged by the Information Owner within two weeks following a serious data breach or significant update.

12.3 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.

12.4 All staff will receive training as part of their induction programme, as will any new pupils that join an academy.

12.5 All users will be made aware of the disciplinary procedures for the misuse of the network leading to malicious attacks.

13 Security Breach Incidents

13.1 Any individual that discovers a security data breach will report this immediately to the DPO via privacy@wellspringacademies.org.uk and to the local DPL.

13.2 When an incident is raised, the Information Owner will record the following information:

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

13.3 The DPL will take the lead in investigating the breach and will be allocated the appropriate time and resources to conduct this.

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

13.5 The DPL 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 DPL determines that the severity of the security breach is low, the incident will be managed in accordance with the following procedures:

13.8 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.

13.9 The Information Owner will issue disciplinary sanctions to the pupil or member of staff.

- 13.9.1 **[Localised deployments only *In house IT Service Provider]** In the event of any external or internal breach the data controller 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.

- 13.9.2 **[Centralised deployments only *IT Service Provider]** The data controller will work with the third-party provider to provide an appropriate response to the attack, including any in-house changes.

13.10 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.

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

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

13.12 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.

13.13 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 school's systems are safe to use.

14 **Assessment of Risk**

The Trust Breach Management Plan provides a framework for the assessment of risks associated with a data breach. It also outlines next steps and reportable breaches.

15 **Consideration of further notification**

15.1 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 15.8 onwards for specific GDPR requirements about personal data).

15.2 The Trust will decide whether notification will help the Trust meet its security obligations under the seventh data protection principle.

15.3 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.

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

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

15.5.1 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.
15.5.2 Specific and clear advice on the steps they can take to protect themselves and what the Trust is willing to do to help them.
15.5.3 A way in which they can contact the Trust for further information or to ask questions about what has occurred.

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

15.7 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:

15.8 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.

15.9 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.

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

15.10.1 The nature of the personal data breach including, where possible.
15.10.2 The type(s), e.g. staff, pupils or governors, and approximate number of individuals concerned.
15.10.3 The type(s) and approximate number of personal data records concerned.
15.10.4 The name and contact details of the data controller or other person(s) responsible for handling the Trust's information.
15.10.5 A description of the likely consequences of the personal data breach
15.10.6 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 data controller will establish the root of the breach, and where any present or future risks lie.

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

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

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

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