Shaw Education Trust

We believe, you achieve

Data Security Policy

Physical security arrangements

1. Site security

1.1 All staff members will act in accordance with the Academy's security policies.

1.2 During Academy events, all rooms except those required will be locked. Only the site manager, or other designated persons, will have a copy of the keys required to access the rooms.

1.3 Unless needed, all paperwork and equipment will be securely stored away.

1.4 When the Academy site is open for events, the event organiser and data expert will carry out an extensive risk assessment to ensure the security of data.

1.5 All Academies will implement a clear desk policy under which personal and sensitive data will not be kept in plain view, such as employee's keeping paperwork which contains pupil information on their desk.

1.6 Any paper documents containing sensitive or confidential information will be securely stored using a lock. Only the relevant member of staff will have a copy of the key required to access the data. This member of staff is responsible for ensuring the security of this key.

1.7 Each Academy is responsible for maintaining an up-to-date record of any key holders.

1.8 Where Academy devices are used at home, a record of all devices taken off the Academy site will be maintained.

2. Devices and equipment

2.1. When using devices such as hard drives to store data, the device will be approved and encrypted by the ICT support team prior to use.

2.2. Devices will be locked and secured when not in use, ensuring that access to data is password protected.

2.3. All electronic equipment is stored in a secure location at the end of each day.

2.4. After using Academy equipment, staff members are responsible for ensuring that it is returned to the appropriate storage location and secured.

2.5. Staff, pupils, parents, visitors and contractors are responsible for their personal belongings, and any data stored on their devices, and the Academy is not liable for any damage or loss which may occur.

2.6. Any equipment which someone wishes to take off the Academy site will be approved by the Principal, in line with the Academy's Personal Devices Policy, in advance and a record of the loan kept.

2.7. Where the security of equipment storing data has been breached, the Academy's data expert will be immediately informed. The expert will then report the incident to the Trust's DPO, where necessary to do so.

E-security arrangements

1. Secure configuration

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

1.2. Any changes to the IT hardware or software will be documented using the inventory, and will be authorised by the ICT support team before use.

1.3. 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.

1.4. Any software that is out-of-date or reaches '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 by suppliers.

1.5. Only cloud computing systems agreed and configured by the ICT support team will be used.

1.6. Each Academy's data expert will ensure that a high-quality filtering system is in place at the Academy.

1.7. All hardware, software and operating systems, including cloud computing, will require passwords for individual users before use.

1.8. Passwords will be changed on a 90 day basis to prevent access to facilities which could compromise network security.

1.9. Passwords will not be written down or stored in a file.

1.10. Staff members will not share private information, such as employee contact details and passwords.

1.11. The Academy believes that locking down hardware, such as through strong passwords, is an effective way to prevent access to facilities by unauthorised users. This is detailed in section 6 of this policy.

1.12. Staff members leaving the Academy will be removed from the Academy's system immediately.

2. Network security

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

2.2. The Academy's firewall will be deployed as a:

- Centralised deployment: the broadband service connects to a firewall that is located within a data centre or other major network location.

2.3. In relation to centralised deployments, the Academy's firewall is managed locally by a third-party, the firewall management service will be thoroughly investigated by the ICT support team, 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.

2.4. In relation to localised deployments, the Academy's firewall is managed on the premises, it is the responsibility of the ICT support team to effectively manage the firewall. The ICT support team will ensure that:

- The firewall is checked regularly 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, do not compromise the overall network security.
- The firewall is checked regularly 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 data expert. The ICT support team will react to security threats to find new ways of managing the firewall.

2.5. In relation to centralised deployments, the Academy 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 Academy's Principal, taking into account the level of security currently provided and any incidents that have occurred.

3. Email usage

3.1. Any emails being sent externally which contain sensitive data, such as those pertaining to safeguarding concerns, will be encrypted to reduce the risk of it being viewed by anyone other than the intended audience.

3.2. The preferred method of encryption is to manually enter 'encrypt' into the subject header before sending the message.

3.3. Encryption is not necessary when sending internal messages due to the security arrangements in place at the Academy, such as the use of firewalls and filtering systems.

3.4. Where sensitive data is sent internally, attachments should be password protected. The recipient(s) should then confirm receipt and request the password either by email, phone or in person. The original attachment sender should be satisfied they are sending the password to the intended recipient. The original sender should not send the password to recipient(s) automatically after the original email.

3.5. Circular emails to parents are sent blind carbon copy (bcc), so email addresses are not disclosed to other recipients.

4. Managing user privileges

4.1. The Academy 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.

4.2. Each Academy Principal will clearly define what users have access to and will communicate this to the ICT support team, ensuring that a written record is kept.

4.3. The ICT support team will ensure that user accounts are set up appropriately such that users can access the facilities required, in line with the Principal's instructions, whilst minimising the potential for deliberate or accidental attacks on the network.

4.4. The ICT support team 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 section 7 of this policy.

4.5. Pupils are responsible for remembering their own passwords; where appropriate to do so, the ICT support team will have an up-to-date record of all usernames and passwords.

4.6. In Primary Academies, KS1 pupils will not have individual logins and class logins will be used instead. If it is appropriate for a pupil to have their individual login, the ICT support team will set up their individual user account, ensuring appropriate access and that their username and password is recorded.

4.7. The 'master user' password used by the ICT support team will be made available to the Principal and will be kept in a secure place.

4.8. A multi-user account will be created for visitors to the Academy, 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 90 day basis, and will be provided as required.

4.9. Academy business managers or Principals should establish robust systems for informing the ICT support team to delete inactive users or users who have left the Academy. The ICT support team will manage this provision to ensure that all users that should be deleted are, and that they do not have access to the system.

5. Monitoring usage

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

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

5.3. An alert will be sent to the ICT support team or appropriate line manager when monitoring usage, if the user accesses inappropriate content or a threat is detected. Alerts will also be sent for unauthorised and accidental usage.

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

5.5. The ICT support team or appropriate line manager will record any alerts using an incident log and will report this to the data expert. All incidents will be responded to in accordance with the Data Protection Policy.

5.6. All data gathered by monitoring usage will be kept in a secure location 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.

6. Removable media controls and home working

6.1. The Academy understands that pupils and staff may need to access the Academy 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.

6.2. The ICT support team will encrypt all Academy-owned devices for personal use, such as laptops, USB sticks, mobile phones and tablets. If any portable devices are lost, this will prevent unauthorised access to personal data.

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

6.4. 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 the Academy's network security. This will be checked by the ICT support team.

6.5. When using laptops, tablets and other portable devices, the data expert will determine the limitations for access to the network, as described in section 6 of this policy.

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

6.7. The ICT support team will filter the use of websites on devices when used onsite, in order to prevent inappropriate use and external threats which may compromise the network security.

6.8. 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.

6.9. The Wi-Fi network at the Academy 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.

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

7. Malware prevention

7.1. The 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.

7.2. The ICT support team will ensure that all Academy devices have secure malware protection, including regular malware scans.

7.3. The ICT support team will update malware protection on a daily basis to ensure they are up-to-date and can react to changing threats.

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

7.5. Filtering of websites, as detailed in section 6 of this policy, will ensure that access to websites with known malware is blocked immediately and reported to the ICT support team.

7.6. The Academy 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.

7.7. The ICT support team will review the mail security technology on a termly basis to ensure it is kept up-to-date and is effective.

Processor protocol

1.1 When handling personal data, staff members **will**:

- Act in accordance with the Academy's Data Protection Policy.
- Verify the identity of the person requesting the information before releasing any data.
- Be cautious about communications which involve phrases such as 'urgent matter', 'forgotten password' or 'computer virus emergency'.
- Report to the Academy data expert any form of intimidation for data from 'higher level management' and where the requester is 'name dropping' to give the appearance that they are authorised personnel.
- Verify with the Academy data expert any third-party authorisation before releasing any information.

- Immediately end any communication which they believe to be suspicious.
- Be cautious of popup windows, mail attachments and suspicious looking websites, such as those claiming to offer something for free.
- Treat information in the strictest confidence.
- Only share the information on a need-to-know basis.

1.2 When handling personal data, staff members **will not**:

- Share the information with an unauthorised individual.
- Release data where the requester's identity cannot be verified.
- Share information which requires releasing information that will reveal passwords, serial numbers, financial data or confidential information.
- Open any emails which they believe to be suspicious.
- Use the Academy system to open or send chain letters, as well as spam or hoax emails.
- Enter their personal or sensitive data, such as their password, if someone is stood looking over their shoulder.

1.3 Before sharing data, all staff members will ensure:

- They are allowed to share it.
- That adequate security is in place to protect it.
- Who will receive the data has been outlined in a privacy notice to the data subject.

1.4 Third-party data processors are bound by the same data requirements as the Trust and, therefore, are expected to act in accordance with the processes and responsibilities outlined in this policy.

Retention and disposal of data

1.1 All data will be retained in line with the Trust's Data Protection Policy and Data Retention Policy, as well as the guidelines provided by the Information and Records Management Society.

1.2 The Trust will apply the principle that electronic data and document will be retained as if they were paper documents.

1.3 Where a piece of electronic data, such as an email, is required to be retained indefinitely, or retained beyond the designated retention period, the data should be printed in hard copy and kept in the appropriate physical document file.

1.4 All hard copies of personal data will be shredded and disposed of once its purpose has been fulfilled.

1.5 Where it is not practical to segregate and manage specific data types uniquely, then a blanket seven year policy will be applied to all data with a prescribed retention period of six years or less.

Staff training and awareness

1.1 Each Academy Principal is responsible for ensuring that data related policies and procedures are effectively communicated to staff members.

1.2 Relevant staff members, such as administrative staff who regularly undertake data processing, will receive training on an annual basis and in regards to any changes in practice or policy.

1.3 All staff members will be made aware of the Trust's data security arrangements as part of their induction training.

1.4 Staff members will undertake cyber-security awareness training as part of their induction training.

1.5 Staff members will receive up-to-date refresher training regarding cyber security and data protection measures on a regular basis.

1.6 In-house training will be provided in each Academy in regards to changes in law and policy, such as GDPR training. The Principal of each Academy is responsible for ensuring that this is undertaken within their establishment.

1.7 All staff members will be made aware of the different methods of social engineering which are most commonly used, including:

- Human-based
- Impersonation – this usually involves a social engineer pretending to be a Academy's employee, board member or technical support in order to gain access to Academy-specific data, such as employee contact details. This can happen over the phone, in person or via email.
- Third-party authorisation – where a social engineer has obtained the name of someone in the Academy and says that they have been granted access to specific information.
- 'Shoulder surfing' – this is when someone is stood looking over an individual's shoulder whilst they enter data, such as their personal details.

- Computer-based
- Popup windows – this is where a window will appear on the screen, saying something like the individual has lost their internet connection and must re-enter their details.
- Mail attachments – viruses can be hidden in email attachments. These are often given names to entice the individual or a long file name.
- Chain, spam and hoax emails – these types of email are often used to gain individual's email addresses and can contain computer viruses.

1.8 Staff members will understand how to prevent and manage concerns for both computer-based and human-based social engineering.

Monitoring

1.1 The impact of this policy and the associated procedures will be monitored by the DPO.

1.2 Each Academy Principal and data expert is responsible for communicating any concerns in relation to data procedures to the DPO.

1.3 This policy will be reviewed and, where necessary, amended on an annual basis by the DPO, in liaison with Academy data experts.

1.4 Following the reporting of a data breach, the DPO and Academy's data expert will review the security arrangements in place and amend as necessary to avoid recurrence of the breach and improve practice.

Shaw Education Trust

We believe, you achieve

The Lodge
Wolstanton High Academy
Milehouse Lane
Newcastle-under-Lyme
Staffordshire
ST5 9JU

Twitter: @shawedutrust
Tel: 01782 742910
Email: info@shaw-education.org.uk
Online: www.shaw-education.org.uk