Policy Updated 09/03/2022

This policy has been significantly updated by L. Treadway DPO and Andrew Harris, IT Strategy Consultant to the trust.

Policy has been tailored to the trust and its schools in a manner that is considered to be both practical and manageable to achieve.

Greater clarity given to the roles and responsibilities. As schools have third-party IT support providers, the responsibilities of the schools are clearly defined with the IT provider giving support and advise.

Consultation with each school's IT Support Provider undertaken at a meeting held on 27th January 2022.

Trust password policy has been added. Password policy based on advice of National Cyber Security Centre (NCSC).

Data and Cyber-Security Breach Prevention and Management Plan

Last updated: 9th March 2022

Contents:

Statement of intent

The Aspire Educational Trust is committed to maintaining the confidentiality, integrity and availability of its information and ensuring that the details of the finances, operations and individuals within the trust and its schools are only accessible to the appropriate individuals. It is, therefore, important to implement appropriate levels of access, uphold high standards of security, take suitable precautions, and have systems and procedures in place that support this.

The trust recognises, however, that breaches in security can occur. In schools, most breaches are caused by human error, so the trust and its schools will ensure all staff are aware of how to minimise this risk. In addition, because most information is stored online or on electronic devices that can be vulnerable to cyber-attacks, the trust and its schools will ensure there are procedures in place to prevent attacks occurring. To minimise both risks, 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

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

- Computer Misuse Act 1990
- The UK General Data Protection Regulation (UK GDPR)
- Data Protection Act 2018
- National Cyber Security Centre (2018) 'Small Business Guide: Cyber Security'
- National Cyber Security Centre (N.D.) 'Cyber Essentials'
- ICO (2021) 'Guide to the UK General Data Protection Regulation (UK GDPR)'
- ESFA (2021) 'Academy Trust Handbook 2021'

This policy has due regard to the trust and schools' policies and procedures including, but not limited to, the following:

- Online Safety Policy
- Data Protection Policy
- Acceptable Use Policy
- Disciplinary Policy and Procedure
- Behavioural Policy
- Social Media Policy

2. Types of security breach and causes

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. This includes unauthorised people within the trust, e.g. schools where pupils access systems that staff have left open and/or logged in, or where staff access data beyond their authorisation, as can occur in schools where all staff are given admin-level access for ease.

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

Damage to physical systems – involves damage to the hardware in the trust and its schools' ICT systems, which may result in data being inaccessible to the trust and its schools and/or becoming accessible to unauthorised persons.

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

Breaches in security may be caused by the actions of individuals, and may be accidental, malicious or the result of negligence:

- Accidental breaches can occur as a result of human error or insufficient training for staff, so they are unaware of the procedures to follow

- Malicious breaches can occur as a result of a hacker wishing to cause damage to the trust and its schools through accessing and altering, sharing or removing data
- Breaches caused by negligence can occur as a result of a staff member knowingly disregarding school policies and procedures or allowing pupils to access data without authorisation and/or supervision

Breaches in security may also be caused by system issues, which could involve incorrect installation, configuration problems or operational errors:

- The incorrect installation of antivirus software, the lack of patch management process and/or use of outdated software can make the trust and its school software more vulnerable to a virus
- Incorrect security settings or incorrect user privilege levels being applied, e.g. unrestricted access to the school network, can allow unauthorised individuals to access the school system
- Operational errors, such as the lack of robust backup procedures resulting in data loss

3. Roles and responsibilities

The DPO is responsible for:

- 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.
- Liaising with the ICT technicians, online safety officers and principals after a data security breach to determine where weaknesses lie and improve security measures.
- Organising training for staff members on data security, network security and preventing breaches.
- Monitoring and reviewing the effectiveness of this policy and communicating any changes to staff members.

ICT technicians are responsible for:

- Liaising with the principal to advise on and agreeing on removing any out-of-date software from the trust and its schools' systems at the earliest opportunity.
- Assisting the principal to make risk-based decisions about actions that may impact on cyber security such as use of personal devices, responding to filtering alerts and the need for more robust back up including Cloud to Cloud.
- Maintaining a robust security posture for schools via effective patch management, perimeter security devices and routine monitoring.
- Installing and reviewing filtering systems for the trust and its schools' networks when appropriate. On some trust sites this responsibility is carried out by the filtering provider and the IT technician is then responsible for reporting on the automated filtering undertaken by the filtering provider such as Schools Broadband.
- Setting up user privileges in line with recommendations from the principal.
- Maintaining an up-to-date and secure inventory of pupil usernames and passwords.

- Maintaining an up-to-date and secure inventory of admin user names and passwords, used to access school/trust systems.
- Liaising with the principal to remove any inactive users from the trust and its schools' systems and ensuring that this is always up-to-date.
- Installing appropriate security software on staff members' personal devices where the principal has permitted for them to be used for work purposes, in line with The Aspire Educational Trust Guidance for Safety in Remote Online Video and Telephone Communication with Pupils and Parents
- Where appropriate, performing a robust offsite back-up of all electronic data held by the trust and its schools, ensuring detailed records of findings are kept. Regular testing of the restore process is required
- Where appropriate, supporting the principal to make a risk-based decision on the need for Cloud to Cloud back-up.
- Ensuring all trust/school-owned devices have secure malware protection and are regularly updated.
- Supporting the principal, where required, to respond to any alerts for access to inappropriate content.
- Supporting the principal with strategic planning for the school's network, systems, processes and software to ensure they remain up to date, supported and secure.

Online safety leads in each school are responsible for:

- Organising training and resources for staff on online safeguarding risks and preventative measures.
- Taking responsibility for online safety within the school and promoting online safety measures to parents.
- Ensuring the relevant policies and procedures are in place to protect pupils from harm, including the Online Safety Policy.
- Monitoring online safety incidents which could result in data breaches and reporting these to the DPO.
- Acting as the named point of contact within the school on all online safety issues.
- Liaising with relevant members of staff on online safety matters, e.g. the principal, DPO, ICT technician and data champion.
- Ensuring staff are aware of their responsibilities to perform back-ups of their electronic data where necessary.
- Ensuring staff are informed of the Cloud based back-up retention periods including Office 365, SharePoint and Google.
- Working with the principal on strategic planning for the school's network, systems, processes and software to ensure they remain up to date, supported and secure.
- Coordinating their school's participation in local and national online safety events, e.g. Safer Internet Day.

Principals are responsible for:

- Ensuring all staff members and pupils are aware of their responsibilities in relation to this policy.
- Contracting IT support providers who have proven cyber security credentials such as Cyber Essential or preferably Cyber Essentials Plus certification.

- Establishing any new user profiles and defining users' access rights for both staff and pupils, communicating these to the ICT technician and maintaining a written record of privileges.
- Making risk-based decisions on the robustness of Cloud based backup systems and considering the need for Cloud to Cloud back up. Financial implications will be the responsibility of the school.
- Receiving alerts and monitoring filtering systems for the school's network.
- Responding to alerts for access to inappropriate content in line with the Online Safety Policy.
- Ensuring there is a maintained inventory of all ICT hardware and software currently used in the school.
- Making an informed risk-based decision on the use of personal devices by staff members. The principal must then recognise the devices will need to become supported with agreement from the member of staff and the IT Support provider. Financial implications from allowing the use of personal devices will be the responsibility of the school.
- Informing the ICT technician of staff members who are permitted to use their personal devices for work purposes so that appropriate security methods can be applied.
- Overseeing any necessary disciplinary actions in response to a data security breach.
- Organising training for staff members in conjunction with the online safety officer, data champion and DPO.
- Strategic planning for the school's network, systems, processes and software to ensure they remain up to date, supported and secure.

The Board of Trustees and Local Academy Committee are responsible for:

- Ensuring that the trust and its schools have IT policies and procedures in place that cover the use of ICT systems and data security, including compliance with the UK General Data Protection Regulations (UK GDPR).
- Monitoring the effectiveness of the trust's policies and procedures relating to data protection and cyber security.
- Supporting the principals and other relevant staff in the delivery of this policy.
- Monitoring implementation of cyber security and data protection onboarding checklists for new schools joining the trust.

All staff members are responsible for:

- Understanding their responsibilities in regard to this policy.
- Reporting any unusual or concerning activity observed on the accounts or devices they use.
- Reporting data breaches.
- Undertaking the appropriate training.
- Ensuring they are aware of when new updates become available and how to safely install them.
- Installing new updates promptly or seeking advice from the school's ICT Technician or Online Safety Lead.
- Setting and securely storing their passwords in accordance with the trust's password policy.

4. Secure configuration

An inventory will be kept of all ICT hardware and software currently in use at each school or in the trust's central team, including mobile phones and other devices provided by the school or trust. The inventory will be stored in the school or trust office and will be audited on a termly basis to ensure it is up-to-date. Any changes to the ICT hardware or software will be documented using the inventory and will be configured by the ICT technician before use.

All systems will be audited regularly by the ICT technician 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. Any software that is out-of-date, reaches or is approaching its 'end of life' will be discussed with the principal to plan for its removal from systems, e.g. when suppliers end their support for outdated products, meaning that the product is not able to fulfil its purpose anymore. Implications for the current users of the software must be considered when planning for removal.

All hardware, software and operating systems will require passwords from individual users. Passwords will be changed, when necessary, to prevent access to facilities which could compromise network security. The trust believes that locking down hardware, such as through the use of strong passwords, is an effective way to prevent access to facilities by unauthorised users. Passwords will need to adhere to a specific character length, use special characters, and not be obvious or easy to guess, in line with the trust's policy on passwords. See Appendix A.

The trust and its schools will refer to the five security controls outlined in the National Cyber Security Centre's (NCSC's) 'Cyber Essentials'. These are:

- **Security Devices or Software (i.e. Firewalls)** – Security devices or software function as a barrier between internal networks and the internet. They will be installed on any device that can access the internet, particularly where staff are using public or otherwise insecure Wi-Fi.
- **Secure configuration** – The default configurations on devices and software are often as open as possible to ensure ease of use, but they also provide more access points for unauthorised users. The trust and its schools will disable or remove any unnecessary functions and change default passwords to reduce the risk of a security breach.
- **Access control** – The more people have access to data, the larger the chance of a security breach. The trust and its schools will ensure that access is given on a 'need-to-know' basis to help protect data. All accounts will be protected with strong passwords, and where necessary, two-factor authorisation.
- **Malware protection** – The trust and its schools will protect themselves from malware by installing antivirus and anti-malware software and using techniques such as whitelisting (a cyber-security strategy under which a user can only take actions on their computer that an administrator has explicitly allowed in advance).
- **Patch management** – The trust and its schools will install software updates regularly to minimise the time frame in which vulnerabilities can be exploited. If the manufacturer stops offering support for the software, the trust and its schools will replace it with a more up-to-date alternative as soon as is practically possible.

5. Network security

In line with the UK GDPR, the trust and its schools will appropriately test, assess, and evaluate any security measures put in place on a regular basis to ensure these measures remain effective.

The trust and its schools will employ the relevant security devices (such as Firewalls) and software in order to prevent unauthorised access to the systems.

Localised firewall deployment (as appropriate)

The school's security implementation will be deployed as a localised deployment, which means the broadband service connects to a device such as a firewall that is located on an appliance or system on the school premises, as either discrete technology or a component of another system.

As the school's firewall is managed on the premises, it is the responsibility of the ICT technician to effectively manage the firewall. The ICT technician 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, are checked to ensure that they do not compromise the overall network security.
- Any compromise of security through the firewall is recorded using an incident log and is reported to the DPO. The ICT technician will react appropriately to security threats to find new ways of managing the firewall.

In a number of trust schools, the ICT technician will not manage the firewall as the equipment on site is owned by the provider (Schools Broadband) who manage and update the firewall. When this is the case, the ICT technician is responsible for keeping up to date with any changes made externally by the provider and communicating key information to the school.

6. Malware prevention

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.

ICT technicians will ensure that all trust and school devices have secure malware protection and undergo regular malware scans in line with specific requirements. ICT technicians will update malware protection regularly to ensure it is up-to-date and can react to changing threats. Malware protection will also be updated in the event of any attacks to the trust or its schools' hardware and software.

Filtering of websites, as detailed in the 'User privileges and passwords' section of this policy, will ensure that access to websites with known malware is risk assessed by the school in conjunction with their IT support provider and blocked immediately. IT support providers will provide advice to the principal of the risks associated with using identified websites. The

principal is then responsible for understanding the risks, making decisions on what staff can and cannot access using school devices and clearly communicate their decisions to staff.

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. ICT technicians will review the mail security technology on a regular basis to ensure it is kept up-to-date and effective.

Staff members are only permitted to download apps on any trust or school-owned device from manufacturer-approved stores and with prior approval from the principal or online safety lead. Where apps are installed, ICT technicians will keep up-to-date with any updates, ensuring staff are informed of when updates are ready and how to install them.

7. User privileges and passwords

The trust and its schools understand that controlling what users have access to is important for promoting network security and data protection. User privileges will be differentiated, e.g. pupils will have different access to data and the network than members of staff, whose access will also be role-based.

Principals will clearly define what users have access to and will communicate this to the ICT technician, ensuring that a written record is kept. The ICT technician 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.

All users will be required to change their passwords if they become known to other individuals, in line with the 'Secure configuration' section of this policy. Pupils are responsible for remembering their passwords; however, the ICT technician will have an up-to-date record of all pupil usernames and passwords and will be able to reset them if necessary. The record of all usernames and passwords is encrypted. Only the principal, online safety lead and ICT technician has access to this inventory. Multi-factor authentication (multiple different methods of verifying the user's identity) should be used wherever possible by staff.

Each ICT technician or designated administrator will have their own dedicated administration account that they use when making amendments. This account must be different to their normal user account. Administration account passwords should be made available to the principal and any other nominated senior leader and will be kept securely in the office.

Administration accounts allow the designated user to make changes that will affect other users' accounts in the school, such as changing security settings, monitoring usage, and installing software and hardware.

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

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

The ICT technician will review the password system regularly to ensure it is working at the required level.

8. Monitoring usage

Monitoring user activity is important for the early detection of attacks and incidents, as well as inappropriate usage by pupils or staff. Schools will inform all pupils and staff that their usage will be monitored, as well as how it is being monitored and why, in accordance with the trust's Acceptable Use Policy and each school's Online Safety Policy.

If a user accesses inappropriate content or a threat is detected, an alert will be sent to the designated member of staff. Alerts will also be sent for unauthorised and accidental access. Alerts will identify the user, the activity that prompted the alert, and the information or service the user was attempting to access. The ICT technician will provide support with monitoring alerts as is required.

Alerts will be recorded and reported to the principal, online safety lead and the DPO if appropriate. All incidents will be responded to in accordance with the 'Data security breach incidents' section of this policy, and as outlined in each school's Online Safety Policy.

ICT technicians will ensure that the school's filtering and monitoring provision is setup correctly and the mechanism for reporting access to inappropriate sites is agreed with the principal. Any member of staff or pupil that accesses inappropriate or malicious content will be recorded in accordance with the monitoring process in the 'Data security breach incidents' section of this policy.

All data gathered by monitoring usage will be kept 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

The trust and its schools understand that pupils and staff may need to access the school network from outside the school premises. Effective security management will be established to prevent access to, or leakage of, data, as well as any possible risk of malware.

The ICT technician will encrypt all school-owned devices for staff 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. If there are older school-owned devices that do not allow this, they should be prioritised for replacement. Devices that have not been encrypted should not be taken off the school site if they have personal data stored on them. Where possible schools and their staff will work cloud based to avoid using devices to move data.

Before distributing any trust/school-owned devices, ICT technicians will ensure that manufacturers' default passwords have been changed. A set password will be chosen, and the staff member will be prompted to change the password once using the device. ICT technicians will check trust/school-owned devices regularly to detect any unchanged default passwords.

In line with the trust's Working from Home, and the Pupil Remote Learning Policy, pupils and staff are not permitted to use their personal devices where the school provides alternatives, such as work laptops, tablets and encrypted USB sticks, unless instructed otherwise by the principal. 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 trust or its schools' network security. This will be checked by ICT technicians.

When using laptops, tablets and other portable devices, the principal will determine the limitations for access to the network, as described in the 'Network security' section of this policy.

Staff who use trust/school-owned laptops, tablets and other portable devices will use them for work purposes only, whether on or off trust premises. Staff will avoid connecting to unknown Wi-Fi hotspots, such as in coffee shops, when using any trust/school-owned laptops, tablets or other devices, or when accessing school networks.

ICT technicians will check security software is installed in order to prevent inappropriate use and external threats which may compromise network security when bringing the device back onto the premises. The trust and its schools use tracking technology where possible to ensure that lost or stolen trust/school-owned devices can be retrieved.

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

The Wi-Fi networks at trust schools will be password protected and will only be given out as required. There should be three networks in trust schools, each setup with relevant permission to systems. The three networks should be:

1. The general school network
2. The BYOD network for personal devices
3. A Guest network – this separate network is for any visitors to the school to limit their access to school networks and any other applications which are not necessary for them to access.

10. Home working and remote learning

Staff and pupils will adhere to data protection legislation and the trust's related policies when working remotely.

Staff will receive annual training regarding what to do if a data protection issue arises from any home working or remote learning.

Wherever possible, personal data, in paper format or stored on devices, will not be taken home by staff members for the purposes of home working, due to the risk of data being lost or the occurrence of a data breach. Cloud based options, such as use of SharePoint and One Drive, should be used where possible.

Staff and pupils may be required to use their own devices for the duration of a remote working or learning period. Any user on a personal device will need to access the school system through a proxy, e.g. VPN. Using a shared personal or household device for trust or school

purposes should be avoided where possible; however, the trust understands that this may not always be possible.

Staff and pupils are not permitted to let their family members or friends use any trust/school equipment, in order to protect the confidentiality of any personal data held on the device. Any staff member found to have shared personal data without authorisation will be disciplined in line with the Disciplinary Policy and Procedure. This may also result in a data breach that the trust would need to record and potentially report to the ICO.

Staff who require access to personal data to enable them to work from home will first seek approval from the principal, and it will be ensured that the appropriate security measures are in place by the ICT technician, e.g. secure passwords and anti-virus software.

Staff will be informed that caution should be exercised while accessing personal data if an unauthorised person is in the same room. If a member of staff needs to leave their device unattended, the device should be locked. Trust/school devices will automatically lock after one minute of inactivity to avoid an unauthorised person gaining access to the device. Where staff are using a personal device, they will be advised that a similar function should be implemented.

Personal data should only be transferred to a home device if this is necessary for the member of staff to carry out their role. When sending confidential information, staff must never save confidential information to a personal or household device. Data that is transferred from a work to a home device will be encrypted so that if any data is lost, stolen or subject to unauthorised access, it will remain safe until it can be recovered.

To ensure reasonable precautions are taken when managing data, staff will avoid:

- Keeping personal data on unencrypted hard drives.
- Sending work emails to and from personal email addresses.
- Leaving logged-in devices and files unattended.
- Using shared home devices where other household members can access personal data.
- Using an unsecured Wi-Fi network.

Staff working from home will be encouraged and enabled to go paperless, where possible, as paper files cannot be protected digitally and may be misplaced. If sensitive data is taken off the trust premises to allow staff to work from home, it will be transported securely and never left unattended. The trust and its schools' procedures for taking data off trust premises will apply to both paper-based and electronic data.

When taking physical copies of data, e.g. paper documents and trust/school-owned devices, off the trust premises, staff will sign out the documents at the school office. The physical data will be signed back in when staff return it.

Pupils are not permitted to use trust/school-owned devices or software for activities that do not pertain to their online education, e.g. use of social media, gaming, streaming or viewing content that is not applicable to their curriculum. Pupils are not permitted to download any software onto trust/school devices, unless instructed to and approved by their teacher.

Pupils will not alter the passwords or encryptions protecting school documents and systems put in place by the school. Pupils will not alter or disable any security measures that are installed on school devices, e.g. firewalls, malware prevention or anti-virus software. Pupils will not share any confidential and/or personal information made accessible to them, e.g. VPN passwords, with anyone who is not authorised to view that information.

Pupils that do not use trust/school devices or software in accordance with this policy will be disciplined in line with the Behavioural Policy.

Pupils must report any technical issues to their teacher as soon as possible. Parents and pupils will be encouraged to contact the school's online safety lead if they wish to report any concerns regarding online safety.

Any devices that are used by staff and pupils for remote working and learning will be assessed by ICT technicians prior to being taken to the home setting, using the following checks:

- System security check – the security of the network and information systems
- Data security check – the security of the data held within the systems
- Online security check – the security of any online service or system, e.g. the school website
- Device security check – the security of the personal device, including any 'bring your own device' systems

ICT technicians will provide staff and pupils with details and instructions for accessing the school network that they will be using throughout the duration of the remote working and learning period.

In the event that a staff member or pupil decides to leave the school permanently, all data in any form will be returned on or before their last day.

11. Backing up data

ICT technicians must monitor the backup process and rectify any failures, ideally a process should be implemented to automatically notify IT staff of a backup failure. Each back-up is retained for a minimum of 15 days.

The school must follow the NCSC's guidance on backing up data where necessary, including:

- Identifying what essential data needs to be backed up.
- Storing backed-up data in a separate location to the original data.
- Consider using the Cloud to store backed-up data.
- Refer to the NCSC's Cloud Security Guidance.
- Ensure that restoring data is regularly practised.

Where possible, back-ups are run overnight and are completed before the beginning of the next school day. Only authorised personnel will be able to access back-ups of the trust and its schools' data.

Schools will ensure that offline back-ups are secured and encrypted to ensure they are protected.

12. Avoiding phishing attacks

ICT technicians 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.

Designated individuals who have an additional account with Administrative privileges will avoid browsing the web or checking emails whilst using this account. Two-factor authentication is used on any important or key accounts, such as the principal's or SBM/Bursar's accounts if possible.

Staff will use the following warning signs when considering whether a communication may be unusual:

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

ICT technicians will ensure that an appropriate email filtering system is used to identify which emails would be classed as junk or spam, applied in accordance with the 'Malware prevention' section of this policy. ICT technicians will ensure they advise on the filtering system that best matches the school's requirements and provides adequate protection.

To prevent anyone having access to unnecessary personal information, principals will review their school's social media accounts and websites on a termly basis, making sure that only necessary information is shared. The DPO will monitor schools' websites and social media accounts on an annual basis, making sure that only necessary information is shared. The principal and the school's data champion will ensure the school's Social Media Policy includes expectations for sharing of information and determines what is and is not appropriate to share.

The principal will ensure parents, pupils, staff and other members of their 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's Acceptable Use Policy.

13. User training and awareness

Principals will arrange training for pupils and staff on, at least, an annual basis to ensure they are aware of how to use the network appropriately, in accordance with the Acceptable Use Policy. This will cover identifying irregular methods of communication 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. Unusual communications could come in a variety of forms, e.g. emails, phone calls, text messages or social media messages.

Online safety leads will arrange for staff and pupils to undertake the appropriate training relating to online safety issues.

The DPO will provide rolling awareness training for staff on aspects of maintaining data security, preventing data breaches, and how to respond in the event of a data breach. This will be achieved through communication with each school's principal who will then liaise with the data champion to ensure awareness training is shared with staff at each trust site. Training for all staff members will be arranged by the principal and school data champion as advised by the DPO within two weeks following an attack, breach or significant update.

Through training in each school, all pupils and staff will be aware of who they should inform first in the event that they suspect a security breach, and who they should inform if they suspect someone else is using their passwords. All staff will receive training as part of their induction programme. All pupils will receive training as part of their curriculum.

A log of any staff training, and attendance should be kept by the school for audit purposes.

All users will be made aware of the disciplinary procedures for the misuse of the network leading to malicious attacks, in accordance with the process detailed in the Behavioural Policy and the Disciplinary Policy and Procedure.

Schools, with support from their ICT technicians, will work towards achieving any mandatory cybersecurity accreditation required of them. The trust will aim for all schools to achieve Cyber Essentials certification over the next 18 months. Schools will be expected to consult their ICT support provider in order to undertake this work which would be in addition to their current contractual agreement.

14. Data security breach incidents

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

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

- 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
- Whether the incident needs to be reported to the relevant authorities, e.g. the ICO or police

The trust's DPO will take the lead in investigating the breach and will be allocated the appropriate time and resources to conduct this. 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. The DPO will oversee a full investigation and produce a comprehensive report. The cause of the breach, and whether it has been contained, will be identified – ensuring that the possibility of further loss or jeopardising of data is eliminated or restricted as much as possible.

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 the AET data breach incident log, and by identifying the user and the website or service they were trying to access
- The principal, where appropriate, will issue disciplinary sanctions to the pupil or member of staff who caused the breach, in accordance with the Behavioural Policy or Disciplinary Policy and Procedure
- In the event of any external or internal breach, the principal will record this using an AET incident log which is then sent to the DPO to agree how it will be responded to appropriately, e.g. by applying security patches, changing usernames and passwords, updating filtered websites or creating further back-ups of information
- The trust and its schools will organise updated staff training following a breach
- Any further action which could be taken to recover lost or damaged data will be identified – this includes the physical recovery of data, as well as the use of back-ups

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

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

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

The trust is required to report personal data breaches to the ICO if there is a likelihood of risk to people's rights and freedoms. If the DPO decides that risk is unlikely, the breach does not need to be reported; however, the trust will need to justify this decision and document the breach.

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

The UK GDPR recognises that it will not always be possible to investigate a breach fully within 72 hours. The information required can be provided in phases, as long as this is done without undue further delay.

In line with the UK GDPR, the following must be provided to the ICO when reporting a personal data breach:

- A description of the nature of the breach, including, where possible:
  - The categories and approximate number of individuals concerned
  - The categories and approximate number of personal data records concerned
- The name and contact details of the DPO
- A description of the likely consequences of the breach
- A description of the measures taken, or proposed to be taken, to deal with the breach
- A description of the measures taken to mitigate any possible adverse effects, where appropriate

The trust will report a personal data breach via the ICO website. The trust will also make use of the ICO's self-assessment tool to determine whether reporting a breach is a necessary next step.

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 without undue delay.

Where the trust or its schools have been subject to online fraud, scams or extortion, the DPO will also report this using the Action Fraud website.

The DPO and ICT technician will test all systems to ensure they are functioning normally, and the incident will only be deemed 'resolved' when it has been assured that the trust and its schools' systems are safe to use.

The trust is aware it must seek permission from the ESFA to pay any cyber-ransom demands in the event of a cyber-crime.

15. Assessment of risks

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, which should record:

- What type of, and how much, data is involved?
- How sensitive is the data? Sensitive data is defined in the UK 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 and/or damage to the trust and its schools' reputation, or risk to the trust and its schools' operations?
- Who could help or advise the trust and its schools on the breach? Could external partners, authorities, or others provide effective support?
- Does the breach need to be reported to the ICO? If so, has it been successfully reported without undue delay?

In the event that the DPO, or other persons involved in assessing the risks to the trust and its schools', are not confident in the assessment of risk, they will seek advice from the ICO.

16. Consideration of further notification

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 data security.

The DPO will assess whether notification could help the individual(s) affected, and whether the individual(s) could act on the information provided to mitigate risks, e.g. by cancelling a credit card or changing a password. In line with the 'Data security breach incidents' section of this policy, if a large number of people are affected, or there are very serious consequences, the ICO will be informed.

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.
- Specific and clear advice on the steps they can take to protect themselves, and what the trust or the school is willing to do to help them.
- A way in which they can contact the school or DPO for further information or to ask questions about what has occurred.

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

17. Evaluation

The DPO will document all the facts regarding the breach, its effects and the remedial action taken. This should be an evaluation of the breach, and what actions need to be taken forward.

The DPO will consider the data and contexts involved, establish the root of the breach, and where any present or future risks lie, taking into consideration whether the breach is a result of human or systematic error and see how a recurrence can be prevented.

The DPO and principals will identify any weak points in existing security measures and procedures. The DPO will work with principals and ICT technicians to improve security procedures wherever required. The DPO and principals will identify any weak points in levels of security awareness and training.

The DPO will report on findings and monitor implementation of the recommendations of the report after analysis and discussion.

18. Monitoring and review

This plan will be reviewed by the DPO regularly according to the AET schedule of policy reviews.

The DPO will be responsible for monitoring the effectiveness of this plan, advising on amending necessary procedures and communicating any changes.

19. Appendix A AET Password Policy

Passwords are a key element in the trust's cyber security prevention plan. Good password discipline can help defeat attempted cyber-attacks. The strongest passwords are hard to guess and not repeated across your different accounts. Passwords need to be complex to withstand brute force attacks. Staff are expected to follow the trust's password complexity rules and the behaviours set out below.

- Wherever possible, use a different password for each account and system.
- **Use a separate password for your work and personal accounts.** School account and e-mail passwords should not be used for any other services such as personal e-mail, social media, Netflix, online shopping etc.
- Do not to use your school email address for personal websites or applications and use a separate unique password for your email accounts as you will often use that email address to reset other passwords.
- Create passwords that are made up of three or four random words that create a memorable image for you. It should preferably be memorable enough for you not to need to write it down. These passwords should be at least 8 characters in length.
- Make sure the random words you choose are not going to be memorable to anyone if momentarily exposed.
- Avoid words from popular fiction.
- Avoid words related to your particular interests and hobbies such as football.
- For key accounts containing high levels of personal data accessed via the internet i.e. MIS, Safeguarding, HR and Finance accounts add complexity by introducing special characters, use character substitution such 3 for E, case changes or start with a lower case or number. These key account passwords should be at least 12 characters in length.
- Never share your password with anyone.
- Always change your password immediately if you believe it has been shared, exposed or breached.
- If you have used the same password for multiple online accounts, you should check to see whether those accounts have ever been compromised through a data breach. You can visit the site www.haveIbeenpwned.com (pronounced p-owned) to find out if your email address has been involved in a data breach and whether your password for that account was exposed. If you discover some of your accounts have been breached, you should reset your passwords for these accounts and any others where you have used the same password.
- Using the same password all over the internet for your accounts makes you vulnerable. For example, if that one password is stolen all your accounts can be accessed. It's good practice to use different passwords for the accounts you most care about. Remembering lots of passwords can be difficult, but if you save them in your browser or a password manager, you don't have to.
- If you really do need to write a password down, make sure you lock it away in a secure place or store it in an encrypted format.

- Online service providers are constantly updating their software to keep your sensitive personal data secure, so store your passwords in your browser when prompted. It's quick, convenient and safer than re-using the same password for all your accounts.
- If you really do need to write a password down, make sure you lock it away in a secure place or store it in an encrypted format.
- Staff should check the strength of their passwords using Password Strength Checker | How strong is my password? Test it now! (thycotic.com) or similar. It is advisable to enter a similar example password rather than your actual one.
- **Where available, switch on two-factor authentication for important accounts** Two-factor authentication (2FA) is normally a free security feature that gives you an extra layer of protection online and stops cyber criminals getting into your accounts – even if they have your password. It reduces the risk by asking you to provide a second factor, such as getting a text or code when you log in, to double check you are who you say you are. Check in with the school IT support provider to help you enable 2FA on key school accounts where it is available such as email, banking and social media.
- If authorised to use personal devices for work purposes 2FA should be enabled if possible.
- IT support providers can set up the authenticator to minimise the requirement to go through the additional 2FA layer of security when staff are accessing via the school's network.