Ascend Learning Trust

Cyber Security Policy

|  |  |
| --- | --- |
| Policy Owner: | Head of IT |
| Date of issue: | November 2024 |
| Policy Level:  | Tier 1  |
| Approved by:  | Full Trust Board |
| Next Review: | November 2025 |

Contents

[Introduction 2](#_Toc176166624)

[Linked Policies 2](#_Toc176166625)

[Policy Statement 2](#_Toc176166626)

[Keeping confidential data, confidential 2](#_Toc176166627)

[Use of Devices, both Trust owned and personal 3](#_Toc176166628)

[Safe use of E-mail 4](#_Toc176166629)

[Password Safety and Security 5](#_Toc176166630)

[Transfer data securely 5](#_Toc176166631)

[Further Steps 6](#_Toc176166632)

[Safeguarding 7](#_Toc176166633)

[Reporting 8](#_Toc176166634)

[Disciplinary Action 8](#_Toc176166635)

# Version Control

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Details | Author | Date |
| 1.0  | Policy formation | Kyle Gaskin | 1st September 2024 |
| 1.1  | Wording change – Lock/Logoff to quantify processes | Jeremy Masson (following feedback from DPE) | 30th October 2024 |

# Linked Policies

* Ascend Data Protection Policy
* Ascend Online Safety Policy
* Ascend ICT & AUP Policy

# Introduction

This Ascend Learning Trust Policy applies to Ascend Learning Trust as a whole and to all the schools in the Trust.

It is the responsibility of the Local Governing Body and Headteacher of each school, and the Board of Trustees and CEO for Trust Shared Services, to ensure that everyone adheres to this policy. In implementing the policy and associated procedures the Governing Body, Headteacher and Trust staff must take account of any advice given to them by the ALT Trust IT Lead, the ALT CEO and/or Board of Trustees.

This Policy is subject to the Scheme of Delegation approved for Ascend Learning Trust. If there is any ambiguity or conflict then the Scheme of Delegation and any specific Scheme or alteration or restriction to the Scheme approved by the Board of Trustees, takes precedence.

If there is any question or doubt about the interpretation or implementation of this Policy, the ALT IT Lead should be consulted.

# Policy Statement

The Ascend Learning Trust Cyber Security Policy outlines our guidance, procedures, and provision for ensuring the integrity of all Trust related data and technology infrastructure.

We are increasingly more reliant on our IT Systems and technology in our everyday roles, which inherently increases the risk of cyber events, such as attack or data breach. These of course can come in many forms, such as hacking, malware, phishing, and even human error.

Such an event can cause reputational and financial damage to the Trust; therefore this should be at the forefront of everything we do when utilising the technology at our disposal. There are a number of security measures that are already in place to help mitigate any risks, however this is in constant review as technology and the ever-present threats become more sophisticated.

Cyber security is the responsibility of all Staff and Students, as well as anyone who may be granted temporary access to Trust systems.

# Keeping confidential data, confidential

Our data by its very nature is confidential, it must be treated as such at all times, this data is valuable, and could be damaging if it falls into the wrong hands. Some common examples are:

* Information regarding Staff, Student, Parent, Trustees, Governors and other parties
* Contractual information
* Unpublished financial information

It is the responsibility of everyone to maintain the integrity and protect this data. We have provided instructions within this policy which can help to safeguard this information, mitigate any potential risks or breaches, and what to do in the event of a breach or if they are unsure.

# Use of Devices, both Trust owned and personal

By accessing Trust systems or data, this inherently introduces “risk” to that data. There are a number of ways that we advise all Staff to keep their devices, both personal and Trust owned, secure:

* **Keep all devices password protected**

We employ a 180 day password change policy, and follow the guidance set out by the NCSC employing three random word guidance, with the addition of uppercase, lowercase and special characters. As of 4th September 2023 we will be inviting users to sign up to 2FA (two factor authentication) for Trust e-mail accounts, when used outside of the Trust network or on personal devices. [https://www.ncsc.gov.uk/news/ncsc-lifts-lidon-three-random-words-password-logic](https://www.ncsc.gov.uk/news/ncsc-lifts-lid-on-three-random-words-password-logic)

* **Ensure Anti-Virus software is kept up to date.**

The Trust uses Anti-Virus and reports are run for any “critical” red alert devices that have issues, so these can be resolved rapidly. IT Support will provide advice for Staff to protect their personal devices, however these remain the responsibility of Staff.

* **Make sure devices are never left unattended, or unlocked, and encrypted**

Devices should be set to automatically lock after 15 minutes of inactivity; however we recommend always locking your device or logging off when not in use for a period of time. Staff should lock their device by holding the Windows and L key.

All mobile phones and tablets, whether Trust or Personal should be protected using PIN, Pattern or fingerprint.

* **Installation of updates to browsers and systems as required**

In most cases, these updates are scheduled to happen automatically, please allow devices the time required to successfully complete the update, if you are unsure, or the device seems to be taking too long, please consult IT Support.

* **Use of Remote systems to connect to Trust systems externally**

The Trust provides remote connectivity for Trust owned laptops and provides school specific access where appropriate, through the use of cloud technology or secure remote access.

It is not advisable to “loan” staff your equipment, if this has been assigned to you, furthermore, students are prevented from logging on to Staff based devices, across the Trust.

Please review the Trust Acceptable Usage Policy for further information on use of Trust systems and devices.

# Safe use of E-mail

E-mail forms an important method of communication across the Trust and the world, as such, it is subject to frequent attacks, which become ever more sophisticated. In order to limit the risks posed, we advise all Staff to:

* **Do not open attachments if the content is inadequately explained**

Attachments containing malware, or phishing scams are common place, for example “You should watch this”, or random Invoice titles, and poorly written e-mail content.

* **If unsure, always ask IT Support and report it!**

IT Support deal with many queries on a daily basis, and the chances are, if you have received something suspicious, others might too. If we know about it, we can take steps to remove it from the entire Trust.

* **If it looks suspicious, trust your instinct**

If it looks too good to be true, it probably is! Did you enter a competition for a holiday? Do you have wealthy relatives that have passed away, that would be specifically contacting you through work? No? Then chances are it is phishing or spam.

* **Who is it from?**

Do you recognise the sender? Are there any inconsistencies with how the e-mail is written, or does it not sound like how the person would write? Trust your gut, and report it. E-mails masquerading as legitimate staff are getting more common, if it doesn’t look like someone you know would have written, then it probably isn’t.

* **Be aware of what you are sending, and to whom**

It is advisable to never send personally identifiable information through e-mail, and when it is a requirement, encryption should always be used. Take care in making sure the correct recipient is in the e-mail chain, mistakes can send information not only to Trust email users, but potentially worldwide, its an easy mistake, but one also easily avoided.

The Trust appends all Subject lines of external e-mail with the word [EXTERNAL] and a banner is presented at the top of each e-mail to state the same. Please remember this advice when opening e-mail.

**CAUTION:** This email originated from outside the organization. Do not click links or open attachments unless you recognize the sender and know the content is safe.

Above all else, if you are unsure, report to IT Support immediately.

# Password Safety and Security

We all have multiple passwords for many different applications, websites, services, keeping track of these can be difficult, but is of huge importance. Password leaks can cause not only information leaks, but potentially system wide issues through the introduction of malware etc. We advise that:

* **Password length and complexity**

Passwords must be changed at least once every 180 days, be a minimum of 8 characters, and employ the three random word guidance set by the NCSC. You should use within your passwords uppercase, lowercase, numbers, non-alpha numeric etc. in order to meet complexity requirements. It is best to use passwords that are not easily guess, such as your own name, date of birth etc.

* **Memorise passwords**

Passwords should never be written down. If there is a genuine need to store passwords, these should be done so in a secure manner, stored in a digitally encrypted file, held in a safe etc. and once finished with, destroyed securely.

* **Do not share passwords**

Your password should be unique to you, and should not be shared, doing so can put you and others at risk. If a password for a service needs to be shared, it should be done so securely, using encryption methods available, and destroyed securely when no longer needed.

# Transfer data securely

Removing or transferring data outside of the Trust will always introduce an element of risk, there are a number of controls put in place to ensure the protection and integrity of Trust data at all times. Trust staff must:

* **Avoid the transfer of sensitive data outside of the Trust**

All data should be considered sensitive and confidential to the Trust. If transfer of data is needed, then it should be done with the permission of the appropriate senior manager, with advice from IT Support.

* **If leaving Trust employment**

If you are leaving, any data stored on Trust systems must be checked by the a HR representative prior to any transfer of data taking place. Any potentially sensitive data will be checked and removed.

* **Reporting**

If you believe you may have transferred sensitive data be it accidental or not, you must report this to IT Support, the Trust Data Protection Officer, and your school Data Protection Lead immediately. The Trust Data Protection Officer works closely with the school Data Protection Leads, and has a responsibility to record all breaches in data security and where required to report these to the ICO (Information Commissioner's Office).

The Trust prevents the use of USB storage devices and printing to non-Trust based printers, this helps to reduce the possibilities of data leak, and the introduction of potentially infected USB devices.

If you believe you have compromised systems or data in anyway, it is your responsibility to inform IT Support, the Trust Data Protection Officer, and your school Data Protection Lead immediately.

# Further Steps

The Trust take as many precautions as reasonably possible to prevent and mitigate the risks relating to cyber security, these include:

* **Starters and Leavers**

All Starters will be automatically created on Trust systems when added to the schools MIS, Arbor by HR. This ensures Safer Recruitment steps have been followed, and that accounts are created with the correct details, these will then be enabled by IT Support when the new starter visits a member of the team. Leavers will be automatically disabled when they reach their contract end date, as input within Arbor by HR.

* **Preventing data leaks**

As previously detailed, the Trust blocks the use of USB storage devices to prevent the transport of data in and out of Trust systems. To this end, printing to remote/home printers is prevented.

* **Encryption**

All Staff laptops are encrypted using BitLocker, utilising a USB stick that acts as the encryption key to start the device. This should always be kept away from the laptop.

* **Lock or Logoff**

This simple step can prevent unauthorised use of your account and details, and should always be done when leaving your desk or room.

* **Reporting**

If a problem isn’t known, steps cannot be taken to rectify it and prevent further damage. Always report incidents where you believe data maybe compromised, loss, theft or damage of a device, suspicious behaviour or activity, potential fraudulent e-mail or attack. This list is not exhaustive, we encourage you to report or seek the advice of IT Support if ever unsure.

* **Safe Internet Use**

Do not attempt to navigate to inappropriate sites, or download suspicious and potentially illegal software. All software installations are managed by IT Support. If you believe a site to be blocked in error, do contact IT Support.

* **Remote / Home Workers**

The Trust provides devices for all Staff that require one as part of their role, as such, this device is encrypted and setup to access Trust systems through the use of a secure VPN. As such, all guidance within this document applies the same as if they were on-site. Access is restricted to United Kingdom based IP addresses only, as recommended by NCSC and DfE.

In addition to the above, Trust IT Support will also ensure:

* **All appropriate safeguards are taken to prevent the unauthorised use of or compromise of Trust systems, through use of firewalls, anti-virus, anti-phishing simulation, regular penetration testing etc. This list is non exhaustive.**
* **Ensure that Staff have access to training materials and know who to contact in the event of a potential incident**
* **Advise of any potential new threats, and investigate them thoroughly**
* **Regular monitoring of all software to ensure updates and patches are installed in a timely and structured way (requires purchase of Lansweeper)**
* **Challenge unattended devices that are unlocked, and where passwords are found openly accessible, reset that password, and request staff attend an IT Support office to unlock**

All Staff should also comply with the Trust ICT Acceptable Usage Policy.

# Safeguarding

All schools have a statutory obligation to monitor their digital resources, identifying any potential threats to the welfare and wellbeing of all Students and Staff.

All Trust schools utilise Surfprotect provided by Exa networks, the Trust Internet provider. Surfprotect is a member of the IWF (Internet Watch Foundation). Traffic is routinely monitored and filtered, and threats reported to IT Support. Safeguarding issues are ported to DSLs within schools, for appropriate action

The Trust IT Support regularly review these methods, to further enhance the procedures in place.

All User access is recorded by our Internet provider, access can be traced to individual users and devices for rapid escalation if necessary

# Reporting

If at any point you have concerns, you must report this immediately to a senior member of IT Support, or any of the Data Protection Officers, no matter how trivial you think it may be.

|  |  |  |  |
| --- | --- | --- | --- |
| School  | Staff member  | Role  | Contact details  |
| Ascend Learning Trust | Rich Corry | Secondary Educational Director | RCorry@ascendlearningtrust.org.uk |
| Royal Wootton Bassett School | Zach Ishani | E-development & Digital Lead | zishani@rwba.ascendlearningtrust.org.uk |
| Lawn Manor Academy | Marek Koza | Assistant Headteacher | mkoza@ascendlearningtrust.org.uk |
| Kingsbury Green Academy | Vicki Scott | Office Manager | vscott@kga.ascendlearningtrust.org.uk |
| The Wellington Academy | Vicky Fawdry | Data Lead | victoriafawdry@twa.ascendlearningtrust.org.uk  |
| Wellington Eagles Primary | Helen Price | Office Manager | hprice@ascendlearningtrust.org.uk  |
| Wellington Lions Primary | Denise O’Brien | Office Manager | deniseobrien@wps.ascendlearningtrust.org.uk |
| Normarsh Junior School | Karen Beard | Office Manager | kbeard@njs.ascendlearningtrust.org.uk  |

# Disciplinary Action

We expect all our employees to use caution, and always have cyber security in their minds when using IT resources. Furthermore, it is expected that all employees will follow this policy and those who cause security breaches could face disciplinary action.

Deliberate and serious breach of this policy may lead to the Trust taking disciplinary measures in accordance with the Trust’s disciplinary policy and procedure. Misuse of Trust systems can have a negative impact upon the reputation of the Trust.

In addition, all the digital resources, including but not limited to Telephony, Cloud based systems, Network (including all hardware) and email related resources are provided for business purposes. The Trust maintains the right to monitor all internet and local network traffic, together with the email systems. Specific content will not be monitored unless there is a suspicion of improper use, and will be done so with the correct authorisation.

Examples of deliberate or serious breaches of this policy include:

* Knowingly disclosing personal login information to an unauthorised third party
* Inappropriate disclosure of personal data, in whatever form
* Knowingly installing or attempting to install software on Trust devices that hasn’t been approved by IT which leads to a breach.
* Allowing the use of Trust devices by unauthorised third parties.
* Storing data on insecure media such as removable media that leads to a breach.