Horizons Specialist Academy Trust
Providing infinite opportunities

Horizons Specialist Academy Trust

E-Security Policy

Adopted by Finance, Risk & General Purposes Committee: 15 June 2021
Date of Next Review: May 2022
Responsible Officer: ICT Manager

1. Legal framework

1.1. This policy has due regard to official legislation including, but not limited to, the following:

- The Human Rights Act 1998
- The UK General Data Protection Regulation
- The Regulation of Investigatory Powers Act 2000
- The Safeguarding Vulnerable Groups Act 2006
- The Education and Inspections Act 2006
- The Computer Misuse Act 1990, amended by the Police and Justice Act 2006

1.2. This policy also has due regard to official guidance including, but not limited to, the following:

- The Education Network 'Managing and maintaining e-security/cyber-security in schools' 2014

1.3. The Horizons Specialist Academies Trust (HSAT) will implement this policy in conjunction with our:

- Acceptable Usage Policy
- E-Safety Policy

Horizons Specialist Academy Trust has carefully considered and analysed the impact of this policy on equality and the possible implications for pupils, parents and staff with protected characteristics, as part of our commitment to meet the Public Sector Equality Duty (PSED) requirement to have due regard to the need to eliminate discrimination, advance equality of opportunity and foster good relations.

2. Types of attack

2.1. Malicious technical attacks: These are intentional attacks which seek to gain access to a school's system and data. Often, these attacks also attempt to use the school's system to mount further attacks on other systems, or use the system for unauthorised purposes, and can lead to reputational damage.

2.2. Accidental attacks: These attacks are often as a result of programme errors or viruses in the school's system. Whilst these are not deliberate, they can cause a variety of problems for schools.

2.3. Internal attacks: These attacks involve both deliberate and accidental actions by users and the introduction of infected devices or storage into the school's system, e.g. USB flash drives.

2.4. **Social engineering:** These attacks result from internal weaknesses which expose the school's system, e.g. poor password use.

3. Roles and responsibilities

3.1. The ICT Manager is responsible for implementing effective strategies for the management of risks imposed by internet use, and to keep its network services, data and users secure.

3.2. The ICT Manager is responsible for the overall monitoring and management of e-security.

3.3. The ICT Manager is responsible for establishing a procedure for managing and logging incidents.

3.4. The Chief Executive will hold regular meetings with the ICT Manager to discuss the effectiveness of e-security, and to review incident logs.

3.5. The Chief Executive will review and evaluate this E-security Policy on an Annual basis in accordance with the ICT Manager, taking into account any incidents and recent technological developments.

3.6. The ICT Manager is responsible for making any necessary changes to this policy and communicating these to all members of staff.

3.7. All members of staff and pupils are responsible for adhering to the processes outlined in this policy, alongside the Trust's E-Safety Policy and Acceptable Usage Agreement.

4. Secure configuration

4.1. An inventory will be kept of all IT hardware and software currently in use at HSAT Academies, including mobile phones and other personal devices provided by the school. This will be stored in the main ICT Office and will be audited on an Annual basis to ensure it is up-to-date.

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

4.3. All systems will be audited on a half-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.

4.4. 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.

4.5. All hardware, software and operating systems will require passwords for individual users before use. Passwords will be changed on a termly basis to prevent access to facilities which could compromise network security.

4.6. The Trust 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.

5. Network security

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

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

Localised deployment: the broadband service connects to a firewall that is located on an appliance or system on the school premises, as either discrete technology or a component of another system.

5.3. As the Trust's firewall is managed on the premises, it is the responsibility of the ICT Manager to effectively manage the firewall. The ICT Manager 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 Chief Executive. The ICT Manager will react to security threats to find new ways of managing the firewall.

6. Managing user privileges

6.1. 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.

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

6.3. The ICT Manager 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.

6.4. All users will be required to change their passwords on a termly 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 this becomes known to other individuals.

6.5. Pupils are responsible for remembering their passwords; however, the ICT Support Team will be able to reset them if necessary.

7. Monitoring usage

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

7.2. The HSAT will inform all pupils and staff that their usage will be monitored, in accordance with the Trust's Acceptable Usage Policy and E-Safety Policy.

7.3. The ICT Manager will record any alerts using an incident log and will report this to the Chief Executive All incidents will be responded to in accordance with section 11 of this policy, and as outlined in the E-Safety Policy

7.4. 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.

8. Removable media controls and home working

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

8.2. Pupils and staff are not permitted to use their personal devices where the Trust shall provide alternatives, such as work laptops, tablets or online services, unless instructed otherwise by the Chief Executive.

8.3. 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's network security.

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

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

8.6. The ICT Manager will ensure that filters are in place for the use of websites on these devices, in order to prevent inappropriate use and external threats which may compromise the network security when bringing the device back onto the premises.

8.7. 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.

8.8. The Wi-Fi network at the Trust will be password protected and will only be given out as required. Staff and pupils are permitted where appropriate to use the WI-FI .

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

8.10. Staff must not hold any personal information on a non trust device. This can include staff or student personal information. If it is necessary to keep personal information on a none trust device, guidance must be sought from the trust ICT manager BEFORE the data is stored on the device.

9. Malware prevention

9.1. 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.

9.2. The ICT Manager will ensure that all school devices have secure malware protection, including regular malware scans.

9.3. The ICT Manager will update malware protection on a Weekly basis to ensure they are up-to-date and can react to changing threats.

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

9.5. 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 Manager.

9.6. The Trust 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.

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

10. User training and awareness

10.1. The ICT Manager and Chief Executive will arrange training for pupils and staff on an Annual basis to ensure they are aware of how to use the network appropriately in accordance with the Acceptable Usage Policy and E-Safety.

10.2. Training will also be conducted around any attacks that occur and any recent updates in technology or the network.

10.3. All staff will receive training as part of their induction programme, as well as any new pupils that join the Trust.

10.4. 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 E-Safety and Social Media Policy.

11. Incidents

11.1. In the event of an internal attack or any incident which has been reported to the ICT Manager, this will be recorded using an incident log and by identifying the user and the website or service they were trying to access.

11.2. All incidents will be reported to the Chief Executive, who may issue disciplinary sanctions to the pupil or member of staff, in accordance with the processes outlined in the E-Safety and Social Media Policies.

11.3. In the event of any external or internal attack, the ICT Manager will record this using an incident log and will contact the third party provider to ensure the attack does not compromise any other schools' network security.

11.4. If necessary, the management of e-security at the Trust will be reviewed to ensure effectiveness and minimise any further incidents.

12. Incident Response Team

12.1. A team will be formed to responded to a serious security breach. This team will consist of ;

- ICT Manager
- Head of Finance & Operations
- ICT Support Team
- Any External support as required.

12.2 This team will report to the Chief Executive and Data Protection Officer with an update as to the seriousness of the breach and an update of what if any data has been lost.

12.3 The ICT team will seal the breach and put in place measures to ensure that it will not occur again .

12.4 A report will be produced by the ICT manager detailing how the breach occurred, what went wrong and how to mitigate it happening again in the future.

13. Monitoring and review

13.1. This policy will be reviewed on an annual basis by the ICT Manager and Chief Executive, who will then communicate any changes to all members of staff and pupils