HCAT

Information Security and Acceptable Use Policy

EDUCATE. EMPOWER. INSPIRE.

Contents

HCAT Information Security and Acceptable Use Policy 2

1. Introduction 2
2. Personal Data 2
3. Information Security 2
4. Organisational Security 3
5. Technical Security 3
6. Software Updates, Firewalls, and Anti-virus Software 3
7. Setup and Access to Facilities and Materials 4
8. Encryption 4
9. Internet Access 4
10. Use of Artificial Intelligence 5
11. Cloud Storage 5
12. Downloading Software or Connecting to other Devices 5
13. Use of IT Facilities 5
14. Passwords 6
15. Email 6
16. Portable Media Devices 6
17. Personal use of HCAT Equipment 7
18. Working off Site / Remotely 7
19. Supervision of Pupil / Student Use 7
20. Monitoring 7
21. Confidentiality and Copyright 8
22. Reporting problems with the Computer System 8
23. Information Security Breaches 8
24. Breach of this policy 8

Version Number	Version Description	Date of Revision
1	Original	September 2019
2	Reviewed and Rebranded	September 2025
3	Acceptable use of AI added	January 2026
4	Updated in line with KCSIE 2026	July 2026

HCAT Information Security and Acceptable Use Policy

1. Introduction

This policy aims to support and reinforce HCAT's policies and should be read in conjunction with the following:

- Records Management and Retention Guidelines
- Data Protection and GDPR Policy
- Online Safety Policy
- Code of Conduct
- Privacy notices for staff, students/pupils and parents/carers.

This policy applies to all employees, members, trustees, agency staff, contractors, work experience students and volunteers.

Any questions or concerns about obligations under this policy should be referred to the Trust Data Protection Officer (DPO) – v.harrison@hcacademytrust.education. Any questions relating to the use of Information Technology (IT) should be raised with the IT manager/support team.

The key areas relating to information security covered in this policy include organisational security and how users engage with and operate paper base and computer-based systems and technical security relating to ensuring that systems used have inbuilt security and protection.

2. Personal Data

Data protection is about protecting information about individuals. Personal Data is data which relates to a living person who can be identified either from that data, or from the data and other information that is available.

Even something as simple as a person's name, their birthday or hobbies count as their Personal Data. HCAT's Data Protection Policy provides further information relating to HCAT's obligations outlined in the UK General Data Protection Regulation (UK GDPR). Anyone accessing or processing personal data has to follow strict rules called "data protection principles'' to ensure that information is used fairly, lawfully and transparently.

3. Information Security

Information security is about safeguarding the Personal Data relating to individuals and protecting other information that is confidential or sensitive. Information security is important as it protects HCAT's ability to function and the data that HCAT collects. Having an appropriate level of IT security enables the safe operation of applications and safeguards the technology being used. IT systems are now used extensively in the delivery of teaching and learning, pastoral and professional services and the administration of the trust.

All systems used present challenges as risks can materialise due to lack of effective security and/or due to the working practices of system users. Data breaches often occur due to human and system errors or weaknesses that can lead to unauthorised access to information and data. Whilst IT is a critical resource in keeping data safe, information security is applicable to paper based as well as computerised systems enabling HCAT's operations.

HCAT will ensure that appropriate security measures are in place to prevent unauthorised individuals gaining access to Personal Data and confidential or sensitive information as required by the following:

- The UK General Data Protection Regulation

- Computer Misuse Act 1990
- Human Rights Act 1998
- The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000
- Education Act 2011
- Freedom of Information Act 2000
- The Education and Inspections Act 2006
- Keeping Children Safe in Education
- Searching, screening and confiscation: advice for schools

4. Organisational Security

Appropriate physical security must be in place with visitors being received and supervised at all times in premises where Personal Data and any confidential or sensitive information is processed and stored.

Portable computer equipment (such as laptops, chrome books, iPads, digital cameras, or portable projectors) and any other media used to store data must be securely stored for example in a locked drawer, cupboard and/or room when left unattended.

Papers which contain Personal Data and confidential information must also be locked away in a secure location and never left unattended. Manual filing systems must be held in secure locations and only accessed on a "need-to-know" basis.

Paper records containing all Personal Data or confidential or sensitive information must be disposed of securely in accordance with HCAT's Records Management and Retention Guidelines. Documents must be placed in confidential waste bins stored in a secure location or by ensuring that all documents have been shredded and disposed of securely. Documents containing Personal Data or any other confidential information should never be placed in the general waste.

When printing documents, secure print should be set until ready to release the documents and only accessed by the authorised user. If printing or photocopying on a shared printer, check that nothing has been left behind, including original copies of documents.

When sending information externally, extra care should be taken to ensure that it is being sent to the correct recipient.

5. Technical Security

Computer systems must have user-type profile password controls and, where necessary, audit and access trails to establish that each user is fully authorised. All users will be informed about overall security procedures and the importance of following these.

6. Software Updates, Firewalls, and Anti-virus Software

All HCAT IT devices that support software updates, security updates, and anti-virus products will be configured to perform such updates regularly or automatically. Any personal devices using any of the Trust's network(s) must all be configured in this way.

Users must not circumvent or make any attempt to circumvent the administrative, physical and technical safeguards that have been put in place to maintain and protect Personal Data, information and IT facilities.

7. Setup and Access to Facilities and Materials

Systems will be set up so that protected files are hidden from unauthorised users. Users will be assigned a clearance that will determine which files are accessible to them. Restricted access to protected data will be controlled according to the role of the user.

All users of HCAT IT facilities will have clearly defined access rights to Trust systems, files, and devices. These access rights are either managed by the IT team directly or by the "owner" of any file sharing drives, folders, and documents (e.g., google file sharing.)

Users should not attempt to access systems, files, or devices to which they have not been granted permissions. If access is provided in error, they should alert the IT support team immediately who will also liaise with the DPO to consider whether there has been a data breach.

Users should log out of systems and lock their equipment, when they are not in use to avoid the risk of any unauthorised access. Equipment and systems should be logged out of and closed completely at the end of each working day.

Equipment should be set up so that screens are not visible to other parties, particularly when personal and confidential data and information is being processed.

If you are doing an online presentation to a group of people, minimise your emails and messaging services before sharing your screen with others.

When using video conferencing technology you should make use of privacy and security features. These can include restricting access to meetings using passwords, controlling when people can join the meeting or controlling who is allowed to share their screens. Think about who and how you share the meeting ID or password. Don't click on links or attachments you were not expecting or from meeting attendees you do not recognise.

Users should contact their IT Support Team for any specific guidance on the information security requirements and setup.

8. Encryption

To provide an increased level of system security, all devices and systems must have an appropriate level of encryption as installed by the IT manager/support team.

Staff may only use personal devices to access trust data, work remotely, or take Personal Data or confidential or sensitive information away from HCAT sites if they have been specifically authorised to do so by the Executive Headteacher or a member of the Leadership team.

The use of personal devices will only be authorised if the devices have appropriate levels of security and encryption. All HCAT data and information must be kept secure at all times.

9. Internet Access

The school wireless internet connection is secure and uses the latest industry standard security.

HCAT operates appropriate filtering and monitoring systems to safeguard pupils, staff and Trust systems from harmful content, cyber threats and inappropriate use. Filtering and monitoring arrangements are reviewed regularly, and at least annually, to ensure they remain effective, proportionate and responsive to emerging technologies and safeguarding risks.

10. Use of Artificial Intelligence

The use of AI to bypass, evade, or interfere with IT security measures within the Trust is strictly prohibited. This includes, but is not limited to:

- Using AI tools to access blocked websites or restricted content.
- Attempting to crack passwords, gain unauthorised access, or manipulate school systems.
- Using AI to disguise or encrypt internet activity to avoid monitoring.
- Automating cyberattacks, denial-of-service attempts, or exploiting system vulnerabilities.
- Any misuse of AI to bypass security controls will be considered a serious breach of Trust policy and may result in disciplinary action. The Trust will continuously monitor network activity to detect and prevent unauthorised AI use.

11. Cloud Storage

HCAT has a set of procedures for the automatic backing up, accessing, and restoring of all data held on school systems, including off-site backups, use of “Cloud Based Storage Systems'' (for example Microsoft 365, google apps and google docs) and is aware that data held in remote and cloud storage is still required to be protected. HCAT will ensure that appropriate industry standard controls and encryption are in place by remote /cloud-based data services providers to protect all data.

12. Downloading Software or Connecting to other Devices

Users of HCAT equipment must not use, download, or install any software, app, programme, or service without permission from the IT support team.

Users must not connect (whether physically or by using another method such as Wi-Fi or Bluetooth) any device or hardware to HCAT IT systems without permission.

13. Use of IT Facilities

All users must use HCAT’s systems responsibly. The following is considered unacceptable use of the trust’s IT facilities, and any unacceptable or inappropriate use of systems will be considered under the Code of Conduct and may be subjected to disciplinary action. Users who damage equipment may also be held financially responsible for the cost of repair or replacement.

- Using the trust’s IT facilities to breach intellectual property rights or copyright.
- Using the trust’s IT facilities to bully or harass someone else, or to promote unlawful discrimination.
- Any illegal conduct, or statements which are deemed to be advocating illegal activity.
- Using, transmitting, or seeking inappropriate, or offensive materials.
- Accessing, creating, storing, linking to or sending material that is pornographic, offensive, obscene or otherwise inappropriate.
- Sharing confidential information about the trust, or any members of the trust’s community.
- Connecting any device to trust IT network(s) without authorisation.
- Setting up any software, applications, or web services on the trust’s network(s) without authorisation or creating or using any programme, tool or item of software designed to interfere with the functioning of the IT facilities, accounts or data.
- Gaining, or attempting to gain, access to restricted areas of the network or drives or to any password-protected information, without approval.
- Allowing, encouraging, or enabling others to gain (or attempt to gain) unauthorised access to the trust’s IT facilities.
- Causing intentional damage or neglectful to IT facilities and equipment.

- Removing, deleting, or disposing of IT equipment, systems, programmes or information without permission.
- Accessing, modifying, or sharing data (including Personal Data) to which a user is not required to have access.
- Promoting a private business, unless that business is directly related to the trust.
- Using websites or mechanisms to bypass the trust's filtering mechanisms.
- Intentionally damage, disable, or otherwise harm the operation of systems.
- Excessive downloading of material from the Internet.

This is not an exhaustive list and there may be other examples that may warrant further investigation and consideration for disciplinary action if appropriate.

HCAT's Child Protection and Safeguarding and Online Safety policies contain additional information relating to safeguarding and online safety with acceptable use agreements, that should also be read in conjunction with this policy.

In exceptional circumstances only, where the use of Trust IT facilities is required for a purpose that would otherwise be considered an unacceptable use, exemptions to the policy may be granted at the Executive Headteacher, Principal or Head of School's discretion only.

14. Passwords

All passwords used to access Trust or school systems, including but not limited to Microsoft 365, must meet the minimum password requirements enforced by that system.

Passwords must be at least 8 characters long and must meet complexity requirements by using at least 3 of the following 4 character types: uppercase letters, lowercase letters, numbers and symbols. Passwords must not use common, recognisable or easily guessed information, such as the school name, Trust name, staff names, academic years, seasons, or simple patterns. Users must also avoid predictable changes, such as adding a number, symbol or year to the end of an old password. Passwords should be long, unique and difficult to guess. We recommend using either a secure machine-generated password or a passphrase made from random words.

All users must use multi-factor authentication where it is available, appropriate or required, as this provides an additional layer of protection if a password is compromised. Where multi-factor authentication is not available or appropriate, stronger password controls or alternative protective measures must be used.

Passwords will not be changed on a fixed routine cycle unless there is a specific security reason to do so. In line with Department for Education and NCSC guidance, users must change their password immediately if it is known or suspected to have been compromised.

15. Email

All emails sent should contain name, job title and contact details.

There are a number of considerations when communicating by email as email is not a secure method of communication, and can be easily copied, forwarded and archived. Email has the same permanence and legal status as written hardcopy (paper) documents and may be subject to disclosure obligations in exactly the same way. Email to outside organisations has the same power to create a binding contract as hardcopy documents.

16. Portable Media Devices

Portable devices such as USB drives/HDDS should not be used, and users should make use of the trust's provided cloud storage arrangements. If in exceptional circumstances a portable media is utilised only devices that have been authorised and provided by the Trust should be used and the IT Support Team will protect any portable media device issued with encryption. Any devices that have not been encrypted must not be used.

Personal Data or confidential or sensitive information must not be stored on a portable storage system (such as a USB memory stick, portable hard disk, or personal computer) unless that storage system is encrypted and has been approved for such use.

If a USB stick is found, please pass to an IT Support Team immediately. Do not plug into a computer.

17. Personal use of HCAT Equipment

Personal use of HCAT issued IT equipment is permitted but its use must comply with all other conditions of this policy and all associated HCAT policies. Personal use must not:

- interfere in any way with your duties or those of any other member of staff;
- have any undue effect on the performance of the computer system; and
- be for any commercial purpose or gain unless explicitly authorised by the trust.

18. Working off Site / Remotely

With the move to cloud-based systems, personal data may be accessible remotely. Staff must ensure that only the minimum necessary information is accessed and used for the specific purpose required. Appropriate security measures (such as strong passwords, multi-factor authentication, and secure connections) must be in place when accessing HCAT systems off site.

Critical Personal Data/Special Category Data as outlined in the Data Protection Policy should not be taken off site in paper format save for specific situations where this is absolutely necessary. For example, a teacher organising a field trip might need to take with them information about pupil/student medical conditions (such as allergies and medication). If only eight out of a class of twenty pupils/students are attending the trip, then the teacher should only take the information about the eight pupils/students.

The trip organiser should decide what information needs to be taken, who will be responsible for looking after it and the arrangements for keeping it secure. Any Personal Data taken off site must be returned.

Working on documents containing Personal Data whilst travelling is only permitted in exceptional cases where prior permission has been granted. If working on a laptop on a train for example, you should ensure that no one else can see the laptop screen and devices must never be left unattended.

If hard copy (i.e. paper) records containing any Personal Data or confidential or sensitive information are taken off HCAT sites, then documents must be kept safe and secure at all times.

19. Supervision of Pupil / Student Use

Pupils/students must be supervised at all times when using HCAT computer equipment. When arranging use of computer facilities for pupils/students, you must ensure supervision is available.

Schools need to ensure that there is an Acceptable User Agreement In place for pupils/students and implement the requirements as outlined in the HCAT Online Safety Policy. Supervising staff are responsible for ensuring that these arrangements are enforced.

Supervising staff must ensure they have read and understand the separate guidelines on Online Safety, which pertains to the child protection issues of computer use by students/pupils.

20. Monitoring

Use of HCAT's computer systems, including email account and storage areas provided may be monitored by the trust to ensure compliance with this policy and applicable laws. This may include remote monitoring of an interactive

logon session. In particular, records of sites visited on the Internet by both students and staff are kept; however, usernames and passwords used on those sites are NOT monitored or recorded.

Monitoring may also be used to identify safeguarding concerns, including exposure to harmful content, cyberbullying, online abuse, radicalisation, self-harm related content, exploitation and attempts to circumvent the Trust's filtering and monitoring systems.

HCAT may also use measures to audit use of computer systems for performance and diagnostic purposes.

21. Confidentiality and Copyright

All users are responsible for complying with copyright law and licences that may apply to software, files, graphics, documents, messages, and other material you wish to use, download, or copy. Even if materials on HCAT's computer system or the Internet are not marked with the copyright symbol (©), it should be assumed that they are protected under copyright laws unless there is an explicit permission on the materials to use them.

You must consult a member of the IT Support Team before placing any order of computer hardware or software, or obtaining and using any software you believe to be free, this is to check that the intended use by HCAT is permitted under copyright law (as well as to check compatibility and discuss any other implications that the purchase may have).

22. Reporting problems with the Computer System

It is the role of the IT Support Team to ensure that HCAT's computer systems are working optimally at all times and that any faults are rectified as soon as possible. Any problems should be reported to the IT support team through the ticket system on the Intranet.

If you suspect that your computer has been affected by a virus or other malware, you must report this to a member of the IT Support Team immediately.

23. Information Security Breaches

All security incidents, breaches and weaknesses should be reported to the DPO as outlined in the Data Protection and GDPR Policy.

24. Breach of this policy

Any breach of this policy will be taken seriously and may result in disciplinary action.