Hummersknott Academy Trust

35 – Acceptable User Policy

Review Date: April 2023

Adopted/V1	V2	V3	V4	V5	V6	V7	V8
June 2010	March 2014	Nov 2015	July 2017	July 2018	July 2019	July 2020	Jan 2022

Hummersknott Academy Trust incorporates Hummersknott Academy and Skerne Park Academy and unless otherwise stated this policy applies to all Academies equally.

PURPOSE

Hummersknott Academy Trust continues to invest heavily in Information and Communication Technology. The provision of ICT throughout the Trust is seen as integral to all subject areas and the administrative systems that support the Academies' operations. This document sets out the Trust's policy for acceptable use of these systems by staff and students/pupils and visitors who use our ICT provision.

SCOPE

Privacy

The Trust reserves the right to monitor all activity on Trust networks and systems by all users. All electronic data held on the Trust's systems are the property of the Trust. The Technical Manager and any designated staff can access any data stored on the Trust's systems at any time to ensure the systems are being used appropriately. Also, at the request of the Principal/Headteacher or a Line Manager, the Technical Manager will investigate if there has been a breach of this policy by searching files and communications on the Academies' systems and their hardware/software. Users must not expect nor assume that their Trust files, emails and Internet activities are private.

Use of Trust ICT Systems

Staff, students/pupils and visitors are provided with access to a wide range of ICT provision to enable and assist their work and educational development. By using the Trust's provision all users are agreeing to this acceptable use policy. **When logging on to any computer in either Academy, users are presented with an information message that alerts them to the fact they are bound by the terms in this policy. All users must click OK to show that they agree to the policy before they can continue to use the systems**. All users will be made aware of this facility prior to using the network. This action is considered as further agreement to the terms of this policy. Users are responsible for their own internet activity on the Trust's ICT systems. Any use that contravenes this policy will be dealt with by the standard disciplinary routes and may involve withdrawal of ICT usage privileges and potential disciplinary or legal action. These sanctions will be applied at the discretion of the Principal/Headteacher.

General Guidelines for ICT and Internet Usage

Hummersknott Academy Trust operates in line with the Counter Terrorism and Security Act 2015. Users must not access material of an extremist or radical nature. This type of ICT usage is flagged by computer systems within each Academy.

Below are some general guidelines for staff and students/pupils regarding the use of Trust ICT systems and the Internet. This list is not meant to be exhaustive, but to highlight the key areas of good practice for safe and responsible use of these systems.

- Users must not use obscene or offensive language at any time. This includes graphics and audio or video recordings
- Users must not use Trust ICT systems to harass or bully any other person. Any such activity will be treated the same as physical bullying and be subject to the same anti bullying procedures as outlined in the Trust policy on Anti bullying www.hummersknott.org.uk or www.skernepark.org.uk
- Use of Trust ICT systems to publish or create offensive/inappropriate or politically directed material will be subject to sanctions and/or disciplinary proceedings
- Users must not bring into either Academy any material that would be considered inappropriate on paper. This includes files stored on cloud storage, CD, DVD or any other electronic storage medium

- Under no circumstances should any users of the Trust's ICT systems download, upload or bring into either Academy material that is unsuitable for children or Academies. This includes any material of a violent, racist or inappropriate sexual nature. The transmission, display, storage or promotion of any such material is a violation of the Computer Misuse Act 1990, and possession of certain types of material can lead to police prosecution
- The accessing of social network ICT sites eg Twitter, Facebook is restricted to authorised staff only on the Trust's sites. **No member of staff is to make contact via social media with a current student or former student 18 years and under who has left a Trust school**
- Any such contact may be called into question by the designated officer and/or Principal/Headteacher and may need to be justified
- Users are all given a unique username and password. This password must be kept secret at all times. Staff must change their password at regular intervals to maintain the security of their files and the data that they access. If any user feels their password has been compromised, they must reset their password immediately or see the ICT Support team to have it reset. The ICT Support team does not know any users' passwords and will only reset the password of a user at their own request
- Any activity carried out under your username is your responsibility. It is your responsibility to ensure that you properly log out of the computer when you have finished using it
- Users are responsible for all files that are stored in their storage area and any websites that have been visited by their user account
- Users' storage areas are backed up on a regular basis, however, Hummersknott Academy Trust can not be held responsible for any data loss, therefore it is good practice for users to make a backup of their area
- Users must not use another person's account or attempt in any way to discover their password
- When assessing Trust systems externally, staff must log in through the Trust managed systems using their school login details
- Users may not use any of the Trust's ICT systems for financial gain, political or any commercial activity
- Users must not breach the copyright of any materials whilst using the Trust's ICT systems. This includes, but is not exhaustive:
  - Not copying, or attempting to copy, any of the either Academies' software
  - Not copying the work of another user or engaging in plagiarism
  - Not storing any files, which require copyright permission for those that they do not hold the copyright to, in their personal storage area; for example, MP3 files or pictures taken by somebody else
- Any breach of copyright whilst using the Trust's ICT systems is the individual user's responsibility and the Trust cannot accept any liability or litigation for such a breach
- Users must not download, copy or attempt to install any software onto Trust computers
- Any attempt by a user to compromise the security or functionality of the Trust's network and its ICT systems, either internally or externally, will be considered as 'hacking'. It should be noted that 'hacking' is illegal under the Computer Misuse Act 1990 and is prosecutable under law
- When accessing any of the Trust's systems from home or an external location, this policy still applies
- The Trust wishes to encourage all users to use the Internet, however it is provided for Trust business and any non-Trust use of the Internet must be carried out in the user's free time
- The Trust cannot be held responsible for any failed personal financial transaction that may happen whilst using the Trust's ICT systems
- Any attempt to circumvent the Academies' firewall and Internet filtering systems will be treated as a breach of this policy. This includes the use of proxy servers and websites to bypass the Internet filtering system. Such activity will be subject to the standard disciplinary procedures and could mean the removal of access to the Trust's ICT systems or Internet access
- There is a wealth of information on the Internet; however due the accessible nature of the Internet, a lot of material is either illegal or unacceptable. Any user that thinks inappropriate or illegal material is being accessed must report it to their teacher, line manager, E Safety Coordinator or the Technical Manager. Any user found accessing such material will be subject to the Trust's disciplinary procedures
- All internet usage is logged and monitored by the ICT Team

Email Guidelines for Staff

All staff and Hummersknott students are provided with an Academy email address. The use of this account is monitored by the Trust and by authorised support companies. Email is a very powerful communication tool; however the following points are made regarding its safe and proper usage:-

- Wherever possible staff are to avoid using all staff group emails and direct emails to specific required recipients
- Email facilities are provided for staff as a method of enhancing communication of work - related issues. All users will be responsible for the content of the messages they send. Any informal or private use of email must be carried out in the employee's own time
- All email communication can be intercepted at any point between you and the recipient. The safest thing is to assume that sending an email is the same as sending a postcard. Users are reminded that use can be monitored and random checks will be made
- When sending an email, the same care and consideration must be taken as when sending a letter on Academies' Letter Head
- Where there is a concern that a member of staff has misused the email system, action may be taken in line with the Trust's disciplinary procedure
- Email should not replace traditional methods of communication. For example, sensitive managerial issues or issues of a secure nature must be communicated in a face to face environment
- When communicating with students/pupils via email do not under any circumstances, give out your personal email address. Always use your Academy address as we can protect you in the event of any false allegations being made against you. Any communication between staff and students/pupils from a non-Trust email address is not logged by us and therefore is an insecure and inappropriate method of communication
- Emails which are abusive, defamatory or discriminatory in any fashion must not be sent. Any such action will result in disciplinary action
- Staff are not permitted to use Trust's email systems to distribute unsolicited or chain mail. Any such mail that arrives in either Academies' system must be deleted immediately and not circulated
- Staff who receive emails regarding viruses or security threats must forward them to the ICT Team

Formal acknowledgement of the acceptable user policy

Staff/visiting users are asked to sign an agreement to abide by the AUP.

Visitors or temporary members of staff will be alerted to the AUP when they meet the Technical Manager or associate to gain their unique log on information. They will also sign an agreement to abide by the AUP. This will be located in their induction pack held by RES.

This policy is not meant to be exhaustive and should be read in conjunction with the Safeguarding Policy and Procedure, and the Trust Online Safety policy. These can be found at www.hummersknott.org.uk or www.skernepark.org.uk

This policy links with Values 3 – Nothing but the best for all, 4 – Taking Responsibility, 7 – Healthy Lives, and 8 – Moral Compass, of Hummersknott Academy Trust's Vision and Values.

RESPONSIBILITY

This policy will be reviewed and updated where necessary by the Network Manager and Executive Principal and approved for adoption by Community Committee.

PUBLICISING THE POLICY

A copy of this policy will be available on each Academy's website and the X Drive/intranet where applicable. Staff will be advised of amendments to this policy via the Staff Bulletin/Briefing and are expected to familiarise themselves with the content.

POLICY STATUS

This is a non-statutory policy.