Staff ICT and Internet Acceptable Use Policy

(Version 2 : Revised 26 Jun 23)

Adopted by The Hawksmoor Learning Trust	Signature	
	Print Name	
	Date	
	On behalf of the Hawksmoor Learning Trust	

Contents

Definitions

Authorised Person	employees authorised by the THLT (Also referred to as the 'Trust') to perform systems administration and / or monitoring of the ICT facilities
ICT Contractor	this is the external contractor retained to support ITC use across the Trust; currently EasiPC Ltd.
ICT facilities	includes all facilities, systems and services including but not limited to network infrastructure, desktop computers, laptops, tablets, phones (Mobile and land line), music players or hardware, software, websites, web applications or services and any device system or service which may become available in the future which is provided as part of the ICT service Includes personal equipment being used to access a Trust sponsored network or accessing the internet from a Trust site
Materials	files and data created using the ICT facilities including but not limited to documents, photos, audio, video, printed output, web pages, social networking sites, and blogs
Personal use	any use or activity not directly related to the users' employment, study or purpose
Stakeholders	anyone with a legitimate interest in the Trust or the schools within the Trust eg pupils, staff, governors, volunteers, visitors, Trustees and Members
Trust	the THLT or any part there off eg the individual schools, the Trust mini-bus
Trust Site	any Trust or school premises or area being used temporarily, or being visited, on Trust related business
Users	any Stakeholder authorised to use Trust ICT facilities
Writing	means letter, fax or email. Writing does not include a text message.

Introduction

1 The Trust strives to have fully cloud based IT systems to facilitate flexible access from many locations

2 ICT;

- 2.1. is an integral part of the way the Trust works / strives to work,
- 2.2. is a critical resource for key stakeholders,
- 2.3. supports teaching and learning, pastoral and administrative functions of the Trust but
- 2.4. poses risks to data protection, online safety and safeguarding.

Aims

3 This policy aims to;

- 3.1. set guidelines and rules on the use of Trust ICT resources for users,
- 3.2. establish clear expectations for the way users engage with each other online,
- 3.3. support Trust policy on data protection, online safety and safeguarding,
- 3.4. prevent disruption to the Trust through the misuse, or attempted misuse, of ICT systems and resources and
- 3.5. support schools in teaching pupils safe and effective internet and ICT use

Scope

4 This policy covers all users of Trust ICT facilities regardless of location.

5 Breaches of this policy may be dealt with under extant disciplinary policies.

Relevant legislation and guidance

6 This policy refers to, and complies with, the following legislation and guidance:

6.1. Data Protection Act 2018

6.2. The General Data Protection Regulation

6.3. Computer Misuse Act 1990

6.4. Human Rights Act 1998

6.5. The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000

6.6. Education Act 2011

6.7. Freedom of Information Act 2000

6.8. The Education and Inspections Act 2006

6.9. Keeping Children Safe in Education 2018

6.10. Searching, screening and confiscation: advice for schools

Unacceptable use

7 ICT resources must not be used for any purpose that may, or threatens to, bring the Trust, or any Stakeholder, into disrepute.

8 The Trust reserves the exclusive right to determine what;

8.1. is acceptable usage,

8.2. is unacceptable usage and

8.3. what may bring the Trust and / or any Stakeholder into disrepute.

9 Any breach of this policy may result in;

9.1. investigation and

9.2. disciplinary or behaviour proceedings.

10 The following is considered unacceptable use of the Trust's ICT facilities by any user (This list is indicative; it is not exhaustive);

10.1. using the school's ICT facilities to;

10.1.1 breach intellectual property rights or copyright,

10.1.2 bully or harass someone else or

10.1.3 promote;

- unlawful discrimination,
- political causes,
- religious ideals or
- unacceptable / bias causes,

10.2. breaching the school's policies or procedures,

10.3. any illegal conduct, or statements which are deemed to be advocating illegal activity,

10.4. accessing, creating, storing, linking to or sending material that may be;

10.4.1 pornographic,

10.4.2 offensive,

10.4.3 obscene or

10.4.4 otherwise inappropriate,

10.5. activity which;

10.5.1 defames or disparages the Trust, a school, a stakeholder or

10.5.2 risks bringing the Trust, a school or stakeholder into disrepute,

10.6. sharing confidential information about;

10.6.1 the Trust,

10.6.2 a school,

10.6.3 another user or

10.6.4 a stakeholder,

10.7. connecting any device to a site ICT network without approval from authorised person,

10.8. setting up any software, applications or web services on the Trust's or a school network without approval by authorised personnel,

10.9. creating or using any programme, tool or item of software designed to interfere with the functioning of the ICT facilities, accounts or data,

10.10. gaining, or attempting to gain, access to restricted areas of the network, or to any password-protected information, without approval from an authorised person,

10.11. allowing, encouraging or enabling others to gain (or attempt to gain) unauthorised access to the Trust's or a school's ICT facilities,

10.12. causing intentional damage to ICT facilities,

10.13. removing, deleting or disposing of ICT equipment, systems, programmes or information without permission by an authorised person,

10.14. causing a data breach, or a potential breach, by accessing, modifying, or sharing data (including personal data) to which a user has no right of access, or for which there is no relevant authorisation,

10.15. using inappropriate or offensive language,

10.16. promoting a private business, unless that business is directly related to the school,

10.17. using websites or mechanisms to bypass the school's filtering mechanisms.

Exceptions from unacceptable use

11 **Dispensation.**

11.1. **Standing Dispensation.**

11.1.1 The Trust accepts that there will be opportunities for recording pupil activities, work and enthusiastic participation through the capturing of photos, videos and the like.

11.1.2 It is also recognised that there will be occasions where Trust ICT facilities are not available to capture the 'golden moment' but to miss it would be a missed opportunity.

11.1.3 Staff must always use Trust ICT facilities if available but may, if no suitable Trust ICT Facilities are readily available, use personal equipment to capture and record images that may, in other circumstances, compromise this policy.

11.1.4 The capture, and temporary recording of such images, is tolerated under the following conditions;

- there is no suitable Trust ICT equipment available,
- the images are uploaded to a Trust ICT facility;
  - at the earliest opportunity,
  - not later than 24 hours from capture,
  - the images are deleted from the personal device immediately after upload and
  - no copies, electronic, paper or otherwise, are retained and
- the CEO / Head / Head of School is informed immediately that images have been captured and recorded in line with this paragraph.

11.2. **Ad Hoc Dispensation.** Where the use of Trust or school ICT facilities is required for a purpose that may otherwise be considered an unacceptable use, exemptions to the policy may be granted, in advance, in writing for each specific incident, at the discretion of the CEO / Head / Head of School.

12 **Process**.

12.1. Every user who may be taking an action that may compromise this policy must, before taking any action, seek written authority from the CEO / Head / Head of School to do so.

12.2. The user must send an email to the CEO / head / Head of School;

12.2.1 stating why the action is required,

12.2.2 outlining a business / educational case for allowing the action, and

12.2.3 providing a brief assessment of the risks in taking that action.

12.3. No action must be taken until the relevant authorities have been received.

Staff Usage (including trustees, governors, volunteers, and contractors)

13 **Access to school ICT facilities and materials**

13.1. The Finance Director (FD);

13.1.1 is the initial point of contact for all non-routine IT / ITC matters in the Trust and

13.1.2 should be consulted before any non-routine engagement with the IT Contractor.

13.2. The Trust's / school's ICT Contractor manages;

13.2.1 access to the Trust's / school's ICT facilities and

13.2.2 materials for all users including access permissions for;

- Office365,
- email accounts and
- other software packages.

13.3. Trustees, governors and staff will be provided with unique log-in / account information and passwords required accessing the school's ICT facilities.

14 Staff who have access to files they are not authorised to view or edit, or who need their access permissions updated or changed, should contact the ITC Contractor

Use of phones and email

15 The school provides each member of staff with a named email address and, if appropriate, a function related email; this / these email account(s) should be used for work purposes only.

16 All work-related business must be conducted using the email address(es) the trust has provided; personal, non-trust emails must not be used for trust related business as this may compromise GDPR.

17 Staff;

17.1. may share Trust email addresses with parents, external agencies etc,

17.2. must;

17.2.1 not share personal email addresses with parents and / or pupils,

17.2.2 only use Trust email addresses when dealing with stakeholders,

17.2.3 not send any work-related materials using a personal email account,

17.2.4 take care with the content of all email messages, as incorrect or improper statements can give rise to claims for discrimination, harassment, defamation, breach of confidentiality or breach of contract.

18 Email messages are required to be disclosed in legal proceedings or in response to requests from individuals under the Data Protection Act 2018 in the same way as paper documents. Deletion from a user's inbox does not mean that an email cannot be recovered for the purposes of disclosure. All email messages should be treated as potentially retrievable; **do not write anything you would not be prepared to say directly to the recipient's face.**

19 Staff must take extra care when sending sensitive or confidential information by email. Any attachments containing sensitive or confidential information should be encrypted so that the information is only accessible by the intended recipient.

20 If staff receive an email in error, the sender should be informed and the email deleted. If the email contains sensitive or confidential information, the user must not make use of that information or disclose that information.

21 If staff send an email in error which contains the personal information of another person, they must inform the CEO or FD immediately and follow the data breach procedure.

22 Staff must;

22.1. not give their personal phone numbers to parents or pupils,

22.2. not use trust phones for personal business and

22.3. only use phones provided by the school to conduct all work-related business.

23 Staff who are provided with mobile phones as equipment for their role must abide by the same rules for ICT acceptable use as set out this policy.

Use of Teams

24 The Trust has well established Teams structure as part of the Office365 software. This should be used for the storage and sharing of sensitive data.

25 **Personal use**

25.1. Staff are occasionally permitted to use school ICT facilities for personal use subject to certain conditions set out below; personal use of ICT facilities is a 'trust-based system', it must not be overused or abused.

25.2. The Trust may withdraw this privilege at any time or restrict access at its discretion.

26 Personal use is permitted provided that such use;

26.1. does not take place during contact time / teaching hours / non-break time,

26.2. does not constitute 'unacceptable use' as defined above,

26.3. takes place when no pupils are present,

26.4. does not interfere with their jobs or prevent other staff or pupils from using the facilities for work or educational purposes.

27 Staff may not use the school's ICT facilities to store personal non-work-related information or materials (such as music, videos, or photos).

28 Staff should be aware that use of the school's ICT facilities for personal use may put personal communications within the scope of the school's ICT monitoring activities. Where breaches of this policy are found, disciplinary action may be taken.

29 Staff should be aware that personal use of ICT (even when not using ICT facilities) can impact on their employment by, for instance, putting personal details in the public domain, where pupils and parents could see them.

30 Staff should take care to follow the Trust's guidelines on social media and use of email (see Annex A) to protect themselves online and avoid compromising their professional integrity.

Personal social media accounts

31 Members of staff should ensure that their use of social media, either for work or personal purposes, is appropriate at all times.

32 The school has guidelines for staff on appropriate security settings for Facebook accounts (see Annex A).

Remote access

33 The aim is for all Trust & School facilities to become cloud based. The location of access does not diminish the responsibilities required; by logging on remotely, the user accepts that this becomes a 'Trust Site'.

Monitoring of school network and use of ICT facilities

34 The Trust reserves the right;

34.1. to access any Trust or school email at any time with reasonable notice and

34.2. to monitor the use of its ICT facilities and network. This includes, but is not limited to, monitoring of:

34.2.1 internet sites visited,

34.2.2 bandwidth usage,

34.2.3 email accounts,

34.2.4 telephone calls,

34.2.5 user activity / access logs and

34.2.6 any other electronic communications

35 Only authorised ICT staff may inspect, monitor, intercept, assess, record and disclose the above to the extent permitted by law.

36 The Trust monitors ICT use in order to:

36.1. ensure child protection is not compromised,

36.2. obtain information related to school business,

36.3. investigate compliance with school policies, procedures and standards,

36.4. ensure effective school and ICT operation,

36.5. conduct training or quality control exercises,

36.6. prevent or detect crime and

36.7. comply with a subject access request, Freedom of Information Act request, or any other legal obligation

Passwords

37 All users of Trust ICT facilities must;

37.1. set strong passwords for their accounts and

37.2. keep these passwords secure.

38 Users are responsible for;

38.1. the security of their passwords and accounts,

38.2. setting permissions for their accounts and

38.3. the files they control.

39 Members of staff who disclose account or password information may face disciplinary action.

40 Parents or volunteers who disclose account or password information may have their access rights revoked.

41 Password and password reset is controlled and administered by the ICT Contractor.

Software updates, firewalls, and anti-virus software

42 All of the Trust's ICT devices that support software updates, security updates, and anti-virus products will be configured by the ICT Contractor to perform such updates regularly or automatically.

43 Users must not circumvent or make any attempt to circumvent the administrative, physical and technical safeguards used to protect personal data and the Trust's ICT facilities.

44 Any personal devices using the Trust' networks must be configured;

44.1. to protect personal data and

44.2. not to cause harm to the Trust's ICT facilities.

Data protection

45 All personal data must be processed and stored in line with;

45.1. extant data protection regulations,

45.2. best practice and

45.3. the Trust's Data Protection Policy.

Access to facilities and materials

46 All users of the Trust's ICT facilities will have clearly defined access rights to appropriate systems, files and devices.

47 Access rights are;

47.1. determined by Heads / Heads of School against the Teaching & Learning needs of each school and

47.2. implemented and managed by the ICT Contractor.

48 Users should not, or attempt to, access, systems, files or devices to which they have not been granted access. If access is provided in error, or if something a user should not have access to is shared with them, they should alert the ICT Contractor immediately.

49 Users must always log out of systems and lock equipment when they are not in use to avoid any unauthorised access.

50 Unless there is a pressing need to leave equipment on at the end of the day, equipment and systems should always be;

50.1. logged out of and

50.2. closed down completely at the end of each working day.

Encryption

51 The Trust will ensure, via the ICT Contractor, that its devices and systems have an appropriate level of encryption.

52 Trust staff may not use personal devices (including computers and USB drives) to access school data, work remotely, or take personal data (such as pupil information) out of school.

Internet access

53 The school wireless internet connection is secured with appropriate monitoring and filtering mechanisms.

54 It may be possible to access unsuitable or inappropriate sites despite these precautions. Any member of staff who finds he / she can access an inappropriate or unsuitable site should report this to the Head / Head of School immediately who will note this and inform the FD.

Parents and visitors

55 Parents and visitors to the school will only be permitted to use the Trust's Wi-Fi with specific authorisation granted by the Head / Head of School.

56 Authorisation will only be granted if;

56.1. parents are working with the school in an official capacity eg as a volunteer or member of the PTA etc

56.2. visitors need to access the school's Wi-Fi to fulfil the purpose of their visit.

57 Staff must not give the Wi-Fi password to anyone who is not authorised to have it; doing so may result in disciplinary action.

58 The decision on who has what access on a school site rests with the Head / Head of School.

Monitoring and review

59 The Trust and ICT Contractor will monitor the implementation of this policy, including ensuring that it is updated to reflect the needs and circumstances of the school.

60 This policy will be reviewed at the beginning of every school year.

Related policies

61 This policy should be read alongside Trust policies on;

61.1. online safety,

61.2. safeguarding and child protection,

61.3. behaviour,

61.4. staff discipline and

61.5. data protection.

_____ Date: 26 Jun 23

Jonathan Davis

Trust Finance Director

Annex A. Facebook cheat sheet for staff

Don’t accept friend requests from pupils on social media

10 rules for school staff on Facebook

1. Change your display name – use your first and middle name, use a maiden name or put your surname backwards instead
2. Change your profile picture to something unidentifiable, or if not, ensure that the image is professional
3. Check your privacy settings regularly
4. Be careful about tagging other staff members in images or posts
5. Don’t share anything publicly that you wouldn’t be just as happy showing your pupils
6. Don’t use social media sites during school hours
7. Don’t make comments about your job, your colleagues, our school or your pupils online – once it’s out there, it’s out there
8. Don’t associate yourself with the school on your profile (eg by setting it as your workplace, or by ‘checking in’ at a school event)
9. Don’t link your work email address to your social media accounts. Anyone who has this address (or your personal email address/mobile number) is able to find you using this information
10. Consider uninstalling the Facebook app from your phone. The app recognises Wi-Fi connections and makes friend suggestions based on who else uses the same Wi-Fi connection (such as parents or pupils)

Check your privacy settings

Change the visibility of your posts and photos to **‘Friends only’**, rather than ‘Friends of friends’. Otherwise, pupils and their families may still be able to read your posts, see things you’ve shared and look at your pictures if they’re friends with anybody on your contacts list

Don’t forget to check your **old posts and photos** – go to bit.ly/2MdQXMN to find out how to limit the visibility of previous posts

The public may still be able to see posts you’ve **‘liked’**, even if your profile settings are private, because this depends on the privacy settings of the original poster

Google your name to see what information about you is visible to the public

Prevent search engines from indexing your profile so that people can’t **search for you by name** – go to bit.ly/2zMdVht to find out how to do this

Remember that **some information is always public**; your display name, profile picture, cover photo, user ID (in the URL for your profile), country, age range and gender

What do to if…

A pupil adds you on social media

In the first instance, ignore and delete the request.

Block the pupil from viewing your profile.

Check your privacy settings again and consider changing your display name or profile picture.

If the pupil asks you about the friend request in person, tell them that you're not allowed to accept friend requests from pupils and that if they persist, you'll have to notify senior leadership and / or their parents.

If the pupil persists, take a screenshot of their request and any accompanying messages.

Notify the senior leadership team or the head teacher about what's happening.

A parent adds you on social media

It is at your discretion whether to respond. Bear in mind that:

- Responding to one parent's friend request or message might set an unwelcome precedent for both you and other teachers at the school
- Pupils may then have indirect access through their parent's account to anything you post, share, comment on or are tagged in

If you wish to decline the offer or ignore the message, consider drafting a stock response to let the parent know that you're doing so.

You're being harassed on social media, or somebody is spreading something offensive about you

Do not retaliate or respond in any way.

Save evidence of any abuse by taking screenshots and recording the time and date it occurred.

Report the material to Facebook or the relevant social network and ask them to remove it.

If the perpetrator is a current pupil or staff member, Trust mediation and disciplinary procedures are usually sufficient to deal with online incidents.

If the perpetrator is a parent or other external adult, a senior member of staff should invite them to a meeting to address any reasonable concerns or complaints and / or request they remove the offending comments or material.

If the comments are racist, sexist, of a sexual nature or constitute a hate crime, you or a senior leader should consider contacting the police.

Annex B: Acceptable use agreement for staff, governors, volunteers and visitors

Acceptable use of the Hawksmoor Learning Trust facilities and the internet: agreement for staff, governors, volunteers and visitors

Name of staff member / governor / volunteer / visitor: _____

When using the Trust's ICT facilities and accessing the internet in a school, or outside school on a Trust device, I will not:

- Access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or pornographic nature or create, share, link to or send such material.
- Use them in any way which could harm the school's reputation.
- Access social networking sites or chat rooms.
- Use any improper language when communicating online, including in emails or other messaging services.
- Install any unauthorised software, or connect unauthorised hardware or devices to a Trust network.
- Share my password with others or log in to a Trust network using someone else's details.
- Share confidential information about the Trust, a school, its pupils or staff, or other members of the community.
- Access, modify or share data I'm not authorised to access, modify or share.
- Promote private businesses.

I understand that the Trust and / or school will monitor the websites I visit and my use of the school's ICT facilities and systems.

I will take all reasonable steps to;

- ensure that work devices are secure and password-protected, and
- keep all data securely stored in accordance with this policy and the Trust's data protection policy.

I will let the designated safeguarding lead (DSL) and Head know if;

- a pupil informs me they have found any material which might upset, distress or harm them or others, and
- I encounter any such material.

I will always use the Trust's / school's ICT systems and internet responsibly and ensure that pupils in my care do so too.

I will not leave this equipment;

- unattended in a vehicle or
- otherwise unsecure or vulnerable.

Signed: _____ Date: _____

Form to be returned to the TOO and retained in the individual's personal file until no longer relevant.

Annex C: IT Hardware Acknowledgement Agreement

THE HAWKSMOOR LEARNING TRUST

ITC Equipment Acknowledgement

I, **(PRINT NAME)** _____,

acknowledge receipt of my THLT ITC Equipment.

Description: _____

Serial Number: _____

On **(Date)**: _____

I agree to use this equipment in accordance with this and other appropriate Trust policies.

I agree to;

be responsible for the security of this equipment, and

submit it when requested to by a suitable authorised member of staff.

I further agree to return it:

at the end of my employment, or

when requested to by a suitably authorised member of staff, and

in a reasonable condition and in such good order to allow its further use.

I understand that any misuse of this equipment may lead to criminal proceedings and / or disciplinary action being taken against me.

Employee Signature: _____

Date: _____

ITC Equipment issued to person named above:

Date: _____

Issuing person's signature: _____

Print Name: _____

Position in THLT: _____

Form to be returned to the TOO and retained in the individual's personal file until no longer relevant.