HOULTON
SCHOOL

Innovation, Aspiration and Excellence

ICT Acceptable Usage & E-Safety Policy

Policy & Procedure Number	HS011	
School Link	Chloe Buckenham (Vice Principal)	
Principal	Michael McCulley	
Chair of Academy Improvement Management (LG) Board	Johanne Thomas	
Category	ICT	
Authorised By	AIM Board	
Author(s)	Chloe Buckenham	
Last revised by	Chloe Buckenham	Jul 2023
Version	1.6	
Status	Under Review:	
	Approved and Adopted:	✓
Issue Date	JULY 2023	
Next Review Date	JULY 2024	
PRINTED COPIES ARE UNCONTROLLED		

Contents

1. Overview

Houlton School’s Information and Communications Technology (ICT) Acceptable Usage and E-Safety Policy applies to all pupils, staff, Partners and volunteers associated with the school and should be read in conjunction with the Houlton School Safeguarding Policy and KCSIE (2020).

The aims of this policy apply to the 'virtual world' that children and young people will encounter whenever they use ICT in its various forms. For example, we know that the internet has been used for grooming children and young people with the ultimate aim of exploiting them sexually; we know that ICT can offer new weapons for bullies, who may torment their victims via websites or text messages; and we know that children and young people have been exposed to inappropriate content when online which can sometimes lead to their involvement in crime and anti-social behaviour.

2. What is ICT?

Information and Communications Technology is an umbrella term that includes any communication device or application, encompassing: radio, television, mobile phones, tablets, computer and network hardware (including peripherals) and software, as well as the various services and applications associated with them.

ICT is much more than an element of the Computer Science and Computing National Curriculum. It is a tool which our staff and pupils use on a daily basis to enrich our teaching and learning in all subjects. Pupils are often already well versed in the uses of technology in its various forms by the time they reach us. It is our role to equip the young people of today with the skills they need to face the challenges of the increasingly technological world of tomorrow.

3. Our Aim

With the current Government focus on developing Computer Science, we aim to give pupils a balanced experience of:

- Using standard and current applications (word processing, spreadsheets, publication, presentation, digital image, video and sound and manipulation software).
- Effective and safe use of the internet and its associated communication capability.
- The computing elements of how a computer works and how we can program it to do what we want.

The rapidly changing nature of the subject means that it is important that we keep up to date with developing technologies, and as these become available it is our vision to embed these into the curriculum.

4. Current digital technologies

ICT in the 21st century has an all-encompassing role within the lives of children and adults. New technologies are enhancing communication and the sharing of information. Current and emerging technologies used in school and, more importantly in many cases, used outside of school can include:

- the internet;
- text messaging;
- Instant messaging often using simple web cameras;
- social networking sites;
- video broadcasting sites such as YouTube;
- chat rooms;
- blogs;
- podcasting;
- gaming sites;
- music download sites;
- file sharing/torrent sites;
- email on all platforms;
- mobile phones with camera and videos;
- games consoles with internet communication;
- tablets and smart phones with web functionality;
- Virtual Learning Environments (VLEs);
- virtual reality goggles\headsets;
- video conferencing;
- screen capture video;
- flipped learning video.

5. E-Safety Risks

The risks can be summarized under the following headings:

E-Content

- exposure to age inappropriate material – pornography, etc;
- exposure to inaccurate or misleading information;
- exposure to socially unacceptable material, such as that inciting violence, hate or intolerance;

- exposure to extremist material or propaganda.

E-Contact

- grooming, including the use of digital communication leading to all forms of sexual contact;
- the use of digital technology to either create or distribute images of a sexual nature (which can be criminal in its nature).

E-Commerce

- exposure of minors to inappropriate commercial advertising;
- exposure to online gambling or commercial and financial scams.

E-Culture

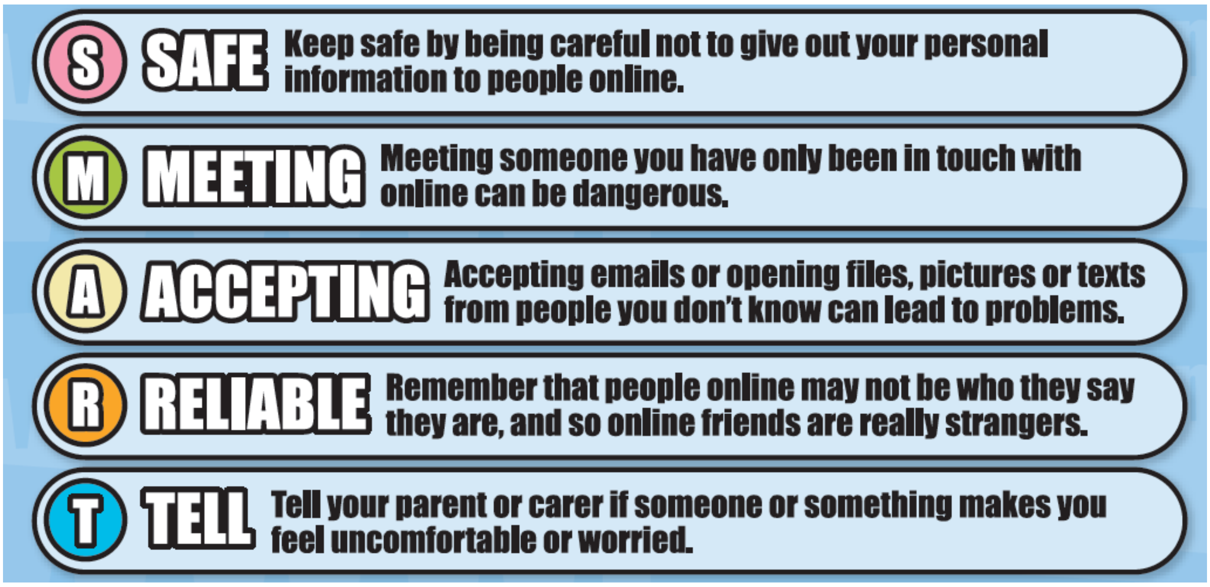
- bullying via mobile phones/social networking/websites or other forms of digital intended to denigrate or humiliate another member of the school community;
- illegal downloading of copyrighted materials, i.e. music and films;
- torrenting or file sharing of copyrighted material (the school will view this as a criminal offence and this will be dealt with accordingly);
- fake news.

E-Video Conferencing

- hijacking of meetings which can be disruptive and disturbing for participants;
- recording meetings without prior agreement.

6. Strategies to minimize E-Safety risks

- E-Safety classroom displays in and around ICT classrooms
- Annual participation in the Houlton School ‘Safer Internet Day’
- E-Safety taught to all pupils through the ICT/Computing and PSRHE curriculum
- Guidance on tackling cyber bullying through pastoral programme
- Sanctions covering use of ICT, through the school’s Positive Behaviour Policy
- Filtering systems to prevent access to inappropriate material
- Policy Central software (automatically generates screen grabs from pupils’ screens when potentially offensive or inappropriate words are detected)
- Surveillance software (Smart-Sync) monitoring all PC use within the school
- Ensuring pupils are aware of the key message of being SMART online



S **SAFE** Keep safe by being careful not to give out your personal information to people online.

M **MEETING** Meeting someone you have only been in touch with online can be dangerous.

A **ACCEPTING** Accepting emails or opening files, pictures or texts from people you don't know can lead to problems.

R **RELIABLE** Remember that people online may not be who they say they are, and so online friends are really strangers.

T **TELL** Tell your parent or carer if someone or something makes you feel uncomfortable or worried.

7. Guidance for video conferencing / live lessons

- Staff should use the waiting room features (therefore controlling who enters the room).
- Passwords or classroom codes must be used and by default there should be a meeting number.
- Control sharing (some applications allow this feature) and provide links directly to participants.
- Where applicable staff should lock the meeting once everyone is present.

8. Reporting

Child protection issues must be reported to the Vice Principal responsible for Child Protection and Safeguarding. E-Safety concerns relating to the use of ICT are reported direct to the Subject Leader for ICT/Computing and, where appropriate, the Assistant Designated Safeguarding Lead (ADSL)/ Vice Principal for Behaviour and Safety. The means to report abuse is available to all members of the school community via CPOMS. Staff will be regularly updated through the school's CPD programme and training for all staff on E-Safety / safeguarding will be provided in line with the Safeguarding Policy.

9. Complaints regarding E-Safety

The school will take all reasonable precautions to ensure E-Safety. However, owing to the global scale and linked nature of internet content, the wide availability of mobile and digital technologies and speed of change, it is not possible to guarantee that unsuitable material will never appear on a school computer or mobile device. Also, the school cannot account for the range of viruses that may cause damage to the device. Neither the school, nor the wider Trust, can accept liability for material accessed, or any consequences of internet access.

Where any complaint relates to the safety of a child, the protocols contained in Safeguarding Policy should be followed.

Where any parent/carer wishes to raise a formal complaint, they should do so by following the process in the school Complaints Policy.

10. Pupil Usage

The computer network is owned by the Transforming Lives Educational Trust and is made available to pupils to further their education at Houlton School. The ICT Acceptable Usage and E-Safety policy has been drawn up to protect everyone. Failure to comply with this policy will result in pupils not being able to use school ICT resources, or more serious sanctions in accordance with Houlton School's Positive Behaviour Policy. Use of the school computer system is contingent upon pupils:

- using the school's ICT provision for school related study purposes only;
- using their own username and password and keeping personal passwords secret;
- logging off when finished using the computer;
- taking responsibility for personal Google Drive accounts and all usage that happens under any login;
- not eating or drinking near a computer or in ICT suites;
- treating the school computers and computer equipment with care and respect at all times and accepting that there will be an expectation to pay for any damage caused by careless use or deliberate abuse;
- not installing or attempting to run any software (on the main computer system or via external hard drives) or re-arranging the hardware under any circumstances;
- understanding that the use of proxy un-blockers or similar system to re-route web traffic is strictly forbidden;
- taking responsibility for the files stored in personal network areas and keeping a back-up of any work which might be important;
- accepting that the school will check personal files and monitor the sites visited and email (including use of Google Classroom);
- understanding that the use of chatrooms, games, social networking sites and playing internet games without the explicit permission of the supervising member of staff is strictly forbidden;

- understanding that the internet will be used to help with school work. Pupils will only enter sites that they have a teacher's permission to enter;
- not using the internet to find information and then submit it as their own work, in accordance with the Joint Council for Qualifications (JCQ) policies on Controlled Assessments and Coursework, and on-screen tests, https://www.jcq.org.uk/;
- not accessing or attempt to download content which would be deemed inappropriate or offensive. This would include but is not limited to, profanities, racist or homophobic language or unkind personal comment about individuals or groups;
- ensuring emails and social media communication is always polite and sensible. Communication with others by email should reflect the rights and responsibilities of other members of the Houlton School community;
- ensuring that they behave responsibly when using Google Classroom or virtual classrooms (whether posting status updates, messaging, emailing or making use of forums);
- not giving out any personal information [like my mobile number, address] online or in emails;
- never arranging to meet anyone that they do not know;
- never creating, transmitting or causing to be transmitted any material which is vulgar, obscene or contains sexually or racially explicit language or material.

11. Use of mobile technology and bring your own devices

Pupils may have access to mobile devices with 4G connectivity. The use of mobile phones is prohibited for pupils at Houlton School except for students in the Sixth Form. Sixth Form students using 4G enabled devices must follow the school's rules regarding the accessing of inappropriate material, which apply regardless of whether pupils are using the internet provided via the school service or mobile data provided via a third party. Any breach of these rules may result in the removal of privileges in the use of the school's ICT resources. Some behaviours can be deemed serious to warrant immediate issuing of further sanctions in line with the Positive Behaviour Policy.

Bring Your Own Device ("BYOD") learning is the use of mobile technology in order to access and leverage the power of internet materials, videos etc for the purposes of engaging and stretching learning. This will be available only to Post 16 students who will be asked to sign and accept the Houlton School BYOD agreement. This policy provides that for Post 16 students:

- It is our intention that students will be able to access learning material via mobile devices in school at the discretion of teachers, subject leaders and pastoral leaders.
- It is the responsibility of all members of the school community to keep all passwords safe at all times.
- Access to the school wifi may be rescinded in cases of inappropriate use.
- USB drives may be connected to school computers if needed, to upload and download work, but it is preferable to use Google Classroom for this purpose. It is the responsibility of the student that any USB drives used on the school computers have been scanned for viruses. The IT technical Department can help with this.

12. Use of Social Media

Rationale

The widespread availability and use of social media applications bring opportunities to understand, engage, and communicate in new and exciting ways. It is important that we are able to use these technologies and services effectively and flexibly. However, it is also important to ensure that we balance this with our duties to our school, the community, our legal responsibilities and our reputation. For example, our use of social networking applications has implications for our duty to safeguard children, young people and vulnerable adults. The policy requirements in this document aim to provide this balance to support innovation whilst providing a framework of good practice. They apply to all members of staff at the school. The purpose of this part of the policy is to:

- Protect the school from legal risks
- Ensure that the reputation of the school, its staff and Partners is protected
- Safeguard all children and vulnerable adults
- Ensure that any users are able to clearly distinguish where information provided via social media is legitimately representative of the school.

Definitions and Scope Social networking applications include, but are not limited to:

- Blogs/Vlogs;
- online discussion forums;
- collaborative spaces;
- media sharing services;
- ‘microblogging’ applications, and online gaming environments.

Examples of social media include: Twitter, Facebook, Windows Live Messenger

Many of the principles of this policy also apply to other types of online presence such as virtual worlds. All members of staff should bear in mind that information they share through social networking applications, even if they are on private spaces, are still subject to copyright, GDPR and Freedom of Information legislation, the Safeguarding Vulnerable Groups Act 2006 and other legislation. They must also operate in line with the school's Equalities, Child Protection and Safeguarding and ICT Acceptable Usage Policies.

Within this policy there is a distinction between use of school-sanctioned social media for professional educational purposes, and personal use of social media.

Personal use of social media

- School staff will not invite, accept or engage in communications with parents/carers or children from the school community in any personal social media whilst employed by or working with Houlton School or the Transforming Lives Educational Trust (TLET).
- Any communication received from children on any personal social media sites must be reported to the Designated Safeguarding Lead.
- If any member of staff is aware of any inappropriate communications involving any child in any social media, these must immediately be reported as above.
- Members of the school staff are strongly advised to set all privacy settings to the highest possible levels on all personal social media accounts.
- All email communication between staff and members of the school community on school business must be made from an official school email account. A Houlton School or TLET email account will be issued to all members of staff both teaching and associate.
- Staff should not use personal email accounts or mobile phones to make contact with parents/carers on school business, nor should any such contact be accepted, except in circumstances given prior approval by the Principal or in an emergency situation.
- Staff are advised to avoid posts or comments that refer to specific, individual matters related to the school and members of its community on any social media accounts.
- Staff are also advised to consider the reputation of the school in any posts or comments related to the school on any social media accounts. Staff must not post any material or comments that bring the school or wider Trust into disrepute.

- Staff should not accept any current pupil of any age or any ex-pupil of the school under the age of 18 as a friend, follower, subscriber or similar on any personal social media account.
- Staff should regularly check their privacy settings.

School-sanctioned use of social media

There are many legitimate uses of social media within the curriculum to enhance and support pupil learning. For example, the school has an official Twitter and Facebook account, and departments may wish to make use of platforms such as Twitter to support the learning of pupils by raising engagement in the subject, providing access to learning and revision materials and also providing support during exam seasons. Some departments may make use of YouTube as a way of recording assessed work – for instance, videoed presentations – so that this may be viewed by visiting exam board moderators. This has been identified as an example of good practice by examination boards.

When using social media for educational purposes, the following practices must be observed:

- Staff should set up a distinct and dedicated social media site or account for educational purposes and must obtain prior consent before doing so from the Principal or Vice principal for Behaviour and Safety. This should be entirely separate from any personal social media accounts held by that member of staff, and ideally should be linked to an official school email account.
- The URL and identity of the site should be notified to the appropriate Head of Faculty and the Vice Principal for Behaviour and Safety before access is permitted for pupils.
- The content of any school-sanctioned social media site should be solely professional and should reflect well on the school.
- Staff must not publish photographs of children without the written consent of parents / carers, identify by name any children featured in photographs, or allow personally identifying information to be published on school social media accounts.
- Care must be taken that any links to external sites from the account are appropriate and safe.
- Accounts must be monitored regularly and frequently (preferably several times a week, including during holidays) by the TLET ICT Services Team. Regular monitoring and intervention is essential in case a situation arises where bullying or any other inappropriate behaviour arises on a school social media account.

- Users of social media should consider the copyright of the content they are sharing and, where necessary, should seek permission from the copyright holder before sharing.
- Users must ensure that their use of social media does not infringe upon relevant data protection laws, or breach confidentiality.
- Where possible, security settings should be set to only allow invited members to comment or publish to any social media feed.
- Staff should not respond to private messages from pupils on any social media site, even where the site is school approved.

We aim to promote positive relationships and the effective use of social media platforms that keep stakeholders informed on updates regarding the school. The school recognises the potential benefits of social media but is aware of the potential harm it can also cause to individuals.

We aim to avoid the promotion of untrue reports and encourage our followers to be mindful of untrue reports. Any account making comments that may be deemed offensive to an individual within the school community, inciting hatred or bringing the school, TLET or any of its academies into disrepute on the school social media forums will be reported to the relevant body and the account blocked.

Any person concerned by or owning an account that raises a discussion point on social media is free to make an appointment to discuss in person at the school. The school will not engage in public discussions over social media.

13. Cloud based applications and services

There are many opportunities for staff and pupils to take advantage of an increasingly wide and diverse range of cloud based tools and services. These include “web applications” and online software packages that provide pupils with access to content creation. Many such services require users to register before access is granted and staff should be wary about the use of any website that requires pupils to provide personal information, or register by way of a social networking service such as Facebook or Twitter.

Houlton School is a *Google Apps for Education* school. This means that every member of staff has access to Google Services via an account provided and managed by the school. School Google accounts provide pupils with a login that does not necessitate them providing any personal information whatsoever. Many cloud services allow users to sign up/register via a Google account and as such, staff should ensure the use of online/cloud based tools is restricted to services that support Google sign in. This would ensure that pupils could register for the service without sharing any personal information.

There may be exceptions to this – such as ucas.com – where personal data is required. Staff should contact the Principal, Vice Principal for Behaviour and Safety or the Head of Faculty for ICT & Computing if unsure.

14. Pupil consequences for misuse of ICT resources

The following are likely to lead to pupils being issued with a consequence. This is meant as a guide and the severity of the consequence will depend on the circumstances in conjunction with the Positive Behaviour Policy.

- Damage to computers or hardware (including headphones, mice, pulling out leads etc.)
- Turning off someone else’s PC/laptop/tablet
- Inappropriate internet access (for offensive content as opposed to games or just being off task)
- Use of email or computer for bullying (posting comments or sending unpleasant emails)
- Use of online platforms for posting inappropriate/offensive material (via forums, status updates, messages or emails), or for cyberbullying

Pupils receiving consequences may have additional sanctions, depending on the nature/severity of the offense and whether or not this is a first offence. These may include:

- Network ban (discretionary, determined by Subject Leader for ICT)
- VLE ban (discretionary, determined by Subject Leader for ICT/E Teaching Staff/LT)
- Phone call/ letter home/ meet with parent/carers
- SLT involvement
- Parents/carers invoiced for damage caused by a pupil
- Internal Refocus work of Fixed Term Exclusion in serious cases.

15. Staff Usage

Laptop usage

- Staff will be assigned a password that will be securely recorded by IT Services. Staff have the ability to alter this. Any devices that use school services such as Outlook for mobile, will require the password to be entered to continue working
- Laptops by law will require software encryption which will be arranged by the IT Team
- All memory sticks must use software encryption
- General usage is covered by the TLET laptop agreement
- Staff should understand pupil policy and ensure that this is upheld when they are responsible for pupils using ICT
- Staff should ensure that they do not allow pupils to use their own staff laptops under any circumstances.

Use of ICT rooms

Staff are responsible for the behaviour of pupils whilst using school ICT resources. All colleagues are expected to be vigilant and ensure that pupils are fully supervised at all times. Specific rules for usage are provided below, but these can be summarised simply with the expectation that staff should leave ICT rooms in the condition that they would expect to find them. Specifically ensuring that staff:

- are fully conversant with the aspects of the school's Positive Behaviour system relating to use of ICT;
- ensure that no equipment is altered, reconfigured or disconnected for any purpose;
- requests for additional or "special" equipment that requires technical support are logged with ICT Technicians at least 48 hours in advance;
- pupils should never enter an ICT classroom without a member of staff present;
- work printed by pupils is not left on desks and that, before printing, pupils have spell-checked their work, used "Print Preview" to ensure that the work prints as expected and have selected the correct printer for the room, ensuring that their name is on their work;
- headphones (if used with permission from supervising staff) are disconnected and returned. Sanitisation protocol will follow the national guidance for schools during and following the COVID-19 pandemic. None should be left out at the

end of the lesson and pupils are on no account allowed to take them out of the room;

- pupils are logged off at the end of the lesson;
- air conditioning/fans are turned off (if used) at the end of the lesson;
- all materials/equipment brought to the room (such as folders, text books, exercise books, worksheets) are removed at the end of the lesson;
- all pupils are carefully monitored at all times and any damage/misuse is reported;
- pupils do not eat or drink in the classroom;
- personal pupil data (such as SEN or disadvantaged student information) must not be displayed while a laptop is connected to a Promethean board;
- for teachers using a room at the end of the day, they must ensure that the equipment is turned off when leaving the room.

16. Monitoring, responsibility and review

The ICT Acceptable Usage / E-Safety Policy will be reviewed annually by the Head of Faculty for ICT / Computing in conjunction with the Vice Principal for Behaviour and Safety / DSL. and Trust IT Central Services.

1. Appendix 1 – ICT Acceptable Use Guide for Pupils: Dos and DON'Ts

DOs	DON'Ts
✓ use the school's ICT provision for school related study purposes ✓ use your own username and password and keep your personal passwords secret ✓ log off when finished using the computer ✓ treat the school computers and computer equipment with care and respect at all times and accept that there will be an expectation to pay for any damage caused by careless use or deliberate abuse ✓ take responsibility for the files stored in personal network areas and keeping a back-up of any work which might be important ✓ understand that the internet will be used to help with school work and that you will only enter sites that you have a teacher's permission to enter ✓ ensure emails are always polite and sensible. ✓ Report any damage to ICT equipment that you notice	☒ Eat or drink near any ICT equipment ☒ Ever share your login details or password ☒ Ever share personal information online unless a teacher or parent / carer has asked you to do so ☒ Leave any computer or device logged in ☒ Use chatrooms, games, social networking sites or internet games without the explicit permission of the supervising member of staff ☒ Use the internet to find information and submit it as your own work ☒ install or attempt to run any software ☒ create, share or cause to be shared any material which is vulgar, obscene or contains sexually or racially explicit language or material. ☒ Damage cause computers or hardware (including headphones, mice, pulling out leads etc.) ☒ Turn off someone else's PC/laptop/tablet ☒ Use email or ICT to bully or be unkind