Heston COMMUNITY SCHOOL

POLICY FOR E-SAFETY AND ACCEPTABLE ICT USAGE

Approved by:	Finance and General Purposes	**Date: 16/06/2026**
Last reviewed on:	March 2026	
Next review due by:	March 2030	

This Policy is founded within our School ethos which provides a caring, friendly and safe environment for all members of our community.

INTRODUCTION

This policy applies to all students, employees, volunteers, workers or self-employed contractors who may have access to, or use of, IT facilities at the School. For employees, adherence to this policy forms part of the School's terms and conditions of employment.

For the purpose of this policy, IT facilities are defined as meaning any of Heston Community School's IT hardware and software, including email, the Internet and other networks, remote access services, and all computers, laptops, iPads or other tablet devices, mobile phones, and any other related applications and devices.

This policy will also apply to:

- Any devices owned by students, parents and visitors which are brought onto the School site
- The use of any new technology being introduced which is not currently detailed in this document.

AIMS

- To ensure safe and appropriate use of the internet and related communication technologies
- To use ICT to deliver the statutory requirements of the curriculum
- To use ICT to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the School's Information Management Systems
- To create an environment in which staff use ICT confidently in their work and students use their ICT skills confidently to enhance their learning.

RISK

Our approach to online safety is based on addressing the following categories of risk:

- **Content** – being exposed to illegal, inappropriate or harmful content, such as pornography, fake news, racism, misogyny, self-harm, suicide, antisemitism, radicalisation and extremism
- **Contact** – being subjected to harmful online interaction with other users, such as peer-to-peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes
- **Conduct** – personal online behaviour that increases the likelihood of, or causes, harm, such as making, sending and receiving explicit images [e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography], sharing other explicit images and online bullying; and
- **Commerce** – risks such as online gambling, inappropriate advertising, phishing and/or financial scams

LEGISLATION AND GUIDANCE

This policy is based on the Department for Education's [DfE's] statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on:

- Teaching online safety in schools
- Preventing and tackling bullying and cyber-bullying: advice for Headteachers and school staff
- Searching, screening and confiscation

It also refers to the DfE's guidance on protecting children from radicalisation. It reflects existing legislation, including but not limited to the Education Act 1996 [as amended], the Education and Inspections Act 2006 and the Equality Act 2010. In addition, it reflects the Education Act 2011, which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for

and deleting inappropriate images or files on pupils' electronic devices where they believe there is a 'good reason' to do so.

LEADERSHIP AND MANAGEMENT

The Network Manager is responsible for ensuring that:

- The School's ICT infrastructure is secure and meets e-safety technical requirements
- The School's password policy is adhered to
- The School's filtering policy is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person
- The Network Team keeps up to date with E-safety technical information
- The use of the School's ICT infrastructure [network, remote access, e-mail, SharePoint etc.] is regularly monitored in order that any misuse or attempted misuse can be reported to the Deputy Headteacher for investigation/action/sanction.
- Any safeguarding concerns relating to online safety must be reported immediately to the Designated Safeguarding Lead [DSL].

MONITORING AND PRIVACY

The School acts in accordance with applicable legislation and the Information Commissioner's Employment Practices Code, notably in relation to the monitoring of communications.

The School undertakes routine monitoring of activity on the IT systems to ensure that these operate correctly and to protect against the risk of harm from viruses, malicious attacks and other known threats. This does not usually involve the monitoring of individual communications or the disclosure of the contents of any user files.

The School reserves the right to monitor all staff and student use of its IT facilities, including emails sent and received, and websites and other online content accessed in order to:

- Ensure the proper safeguarding of students, minimising exposure to violence, pornography, extremist views and risk of radicalisation
- Protect the IT facilities against viruses, hackers and other malicious attack
- Assist in the investigation of breaches of this policy, to prevent or detect crime or other unauthorised use of the IT facilities
- Comply with legal requirements, for example as part of a police investigation or by order of a court of law, or where necessary as part of a disciplinary investigation
- Pursue the School's other pressing academic and business interests; for example by reviewing the emails of employees on long-term sick leave or to disclose documents under the Freedom of Information Act 2000.

In all cases, monitoring of individual staff content shall only be carried out with the authorisation of the Headteacher.

DISCIPLINARY REGULATIONS AND ENFORCEMENT

The School may take disciplinary action against students or staff if their use of the IT facilities are in breach of this policy.

Where any allegation of misuse has been made against a member of staff or student, the School shall have the right to inspect and take copies of any material held in the name of that student or staff member on any of the IT facilities that might provide evidence for or against the allegation.

If a complaint or allegation is received, a member of staff or student's user account may be suspended for investigation. Whenever possible, users will be notified of such suspension.

Penalties for breach of this policy may include temporary or long-term suspension of access to the IT facilities. Other disciplinary penalties may be imposed in accordance with the School's relevant procedures up to and including permanent exclusion in the case of a student, or dismissal in the case of staff. The School may refer the user to the police, where appropriate and will co-operate fully with any investigations.

COMMERCIAL ACTIVITIES

Use of the IT facilities for commercial activities is permitted only by employees of Heston Community School and only when such use forms part of the duties of employment. Any queries on whether a commercial activity using the IT facilities is permitted should be raised with appropriate Line Managers before commencing.

The use of the IT facilities by students for commercial activities is not permitted.

USE OF THE INTERNET

The Internet is an essential element of 21st Century life for education, business and social interaction; the School has a duty to provide students with quality internet access as part of their learning experience.

Internet use is a part of the School Curriculum and a necessary tool for staff and students. Students will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use within their learning. Students will be educated in the effective use of the Internet for research, including the skills of location, retrieval and evaluation; they will be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

The School Internet access will include appropriate filtering. However, if internet research is set for a class activity or homework using specific/suggested websites, these must have been checked by teachers or other relevant staff to ensure that they are suitable. The School will also ensure that the use of Internet derived materials by staff and students complies with copyright law.

USE OF SCHOOL EQUIPMENT

- No personally owned applications or software packages should be installed on to school ICT equipment
- Personal or sensitive data [belonging to staff] should not be stored on the local drives of desktop or laptop PCs. If it is necessary to do so, the local drive must be encrypted
- All staff should ensure any screens are locked [by pressing Windows button and the L key simultaneously] before moving away from a computer during the normal working day to protect any personal, sensitive, confidential or classified data and to prevent unauthorised access.

PASSWORDS

- Passwords or encryption keys should not be recorded on paper or in an unprotected file
- Passwords should be changed at least every three months
- Users should not use the same password on multiple systems or attempt to synchronise passwords across systems
- Students must inform staff immediately if passwords become known to other students or forgotten. Students must see a member of the Network Team or their class teacher to have their password reset.

EDUCATION AND TRAINING

STUDENTS

- E-safety education is provided as part of PSHE and is regularly revisited in ICT and other lessons across the curriculum
- Students are taught in lessons to be critically aware of the materials/content they access on-line and are guided to validate the accuracy of the information
- Students are helped to understand and encouraged to adopt safe and responsible use of ICT, the internet and mobile devices both within and outside of school
- Students are taught to acknowledge the source of information used and to respect copyright when using material accessed on the Internet
- Rules for the use of ICT systems and the Internet are outlined in the *Code of Conduct for Using Computers and Mobile Devices* to be found in every Student Planner

STAFF

- The Deputy Headteacher will ensure that all staff are aware of the procedures that need to be followed in the event of an E-safety incident taking place
- All new staff receive E-safety training as part of their induction programme, ensuring that they fully understand the School's Policy for E-Safety and Acceptable Usage and Safeguarding and Child Protection Policies
- Staff who require additional training can refer to the Child Exploitation and Online Protection [CEOP] website and if further training is required they can speak to the Designated Safeguarding Lead.
- Staff to act as good role models in their use of ICT, the internet and mobile devices.

CYBER-BULLYING

1. Definition

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of 1 person or group by another person or group, where the relationship involves an imbalance of power. [See also the school behaviour policy].

2. Preventing and addressing cyber-bullying

To help prevent cyber-bullying, we will ensure that pupils understand what it is and what to do if they become aware of it happening to them or others. We will ensure that pupils know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.

The school will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Class teachers/form teachers will discuss cyber-bullying with their tutor groups.

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes personal, social, health and economic [PSHE] education, and other subjects where appropriate.

All staff, governors and volunteers [where appropriate] receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training.

In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school behaviour policy. Where illegal, inappropriate or harmful material has been spread among pupils, the school will use all reasonable endeavours to ensure the incident is contained.

The DSL will report the incident and provide the relevant material to the police as soon as is reasonably practicable, if they have reasonable grounds to suspect that possessing that material is illegal. They will also work with external services if it is deemed necessary to do so.

MANAGING INTERNET ACCESS

1. Information system security

- School IT systems, capacity and security will be reviewed regularly. Virus protection will be updated regularly
- The School has IT security systems in place, but cannot guarantee that these will prevent every attempt to access confidential or restricted data. Everyone must ensure that confidential material is password-protected and / or encrypted as appropriate to prevent unauthorised access by third parties.
- No external storage devices (e.g. USB drives or personal laptops) may be connected to the School network without explicit authorisation from the Network Manager.

2. Social networking and personal publishing

- The School will block/filter access to inappropriate social networking sites
- Students will be advised never to give out personal details online which may identify them or their location
- Students and parents will be advised about the risks of using social network spaces outside School
- There must be no contact between staff and students on social networking sites using personal identities
- Any online contact between staff and students must only be through the use of school email addresses or approved, appropriate applications
- Staff are made aware of expectations with regard to their personal use of social media within the general Staff Code of Conduct
- All staff additionally sign the *Policy For E-Safety and Acceptable ICT Usage,* kept in their Personnel Files, to ensure safe practices with regard to the use of the school IT systems, the internet and social networking
- All students will sign the School's Code of *Conduct for using Computers and Mobile Devices* [Appendix A] which reinforces the safe and sensible use of all IT equipment and services including the internet and social media.

3. Managing filtering

- The School will work with its contracted provider of filtering services to ensure systems to protect students are reviewed and improved
- If staff or students discover an unsuitable site, it must be reported immediately to the ICT technical team
- SLT and the ICT technicians will ensure that regular checks are made to ensure that the filtering methods selected are appropriate and robust.

4. Managing emerging technologies

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in School is allowed.

5. Mobile phones

- Students may not use mobile phones on the School site at any time
- The sending of abusive messages or other forms of inappropriate communication is

forbidden
- Student use of mobile phones during the school day will result in confiscation and the imposition of other sanctions, as appropriate
- Mobile phone usage by staff is only permitted in offices or the Staffroom
- Staff may not share their personal mobile phone numbers with students.

6. Personal Devices

- Students in the Sixth Form may use laptops to support their learning
- Privately owned ICT equipment should never be connected to the School's network without the specific permission of the Network Manager
- No removable data storage devices may be connected to the School network in line with the School's GDPR Policy.

7. Protecting personal data

- Personal data will be recorded, processed, transferred and made available according to the UK General Data Protection Regulation [UK GDPR] and the Data Protection Act 2018

8. Handling online safety complaints

- Complaints of IT misuse by students will be dealt with by the AHT in charge of E-Safety
- Any complaint about staff misuse must be referred to the Headteacher
- Complaints of a child protection nature will be dealt with in accordance with School Safeguarding and Child Protection policy.

9. Monitoring and review

- The implementation of this policy will be monitored and evaluated by the Senior Leadership Team
- The policy will be reviewed in line with the LGfL framework; this review will take place every three years or whenever there is a significant change in national guidance on online safety.

10. Examining Electronic Devices

The Headteacher, and any member of staff authorised to do so by the Headteacher, can carry out a search and confiscate any electronic device that they have reasonable grounds for suspecting:

- Poses a risk to staff or pupils, and/or
- Is identified in the school rules as a banned item for which a search can be carried out, and/or
- Is evidence in relation to an offence

Before a search, if the authorised staff member is satisfied that they have reasonable grounds for suspecting any of the above, they will also:

- Make an assessment of how urgent the search is, and consider the risk to other pupils and staff. If the search is not urgent, they will seek advice from the Headteacher / DSL.
- Explain to the pupil why they are being searched, how the search will happen, and give them the opportunity to ask questions about it
- Seek the pupil's cooperation

Authorised staff members may examine, and in exceptional circumstances erase, any data or files on an electronic device that they have confiscated where they believe there is a 'good reason' to do so.

When deciding whether there is a 'good reason' to examine data or files on an electronic device, the staff member should reasonably suspect that the device has, or could be used to:

- Cause harm, and/or
- Undermine the safe environment of the school or disrupt teaching, and/or
- Commit an offence

If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL / Headteacher / other member of the senior leadership team to decide on a suitable response. If there are images, data or files on the device that staff reasonably suspect are likely to put a person at risk, they will first consider the appropriate safeguarding response.

When deciding if there is a good reason to erase data or files from a device, staff members will consider if the material may constitute evidence relating to a suspected offence. In these instances, they will not delete the material, and the device will be handed to the police as soon as reasonably practicable. If the material is not suspected to be evidence in relation to an offence, staff members may delete it if:

- They reasonably suspect that its continued existence is likely to cause harm to any person, and/or
- The pupil and/or the parent refuses to delete the material themselves

If a staff member **suspects** a device **may** contain an indecent image of a child (also known as a nude or semi-nude image), they will:

- **Not** view the image
- Confiscate the device and report the incident to the DSL (or equivalent) immediately, who will decide what to do next. The DSL will make the decision in line with the DfE's latest guidance on screening, searching and confiscation and the UK Council for Internet Safety (UKCIS) guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people

Any complaints about searching for or deleting inappropriate images or files on pupils' electronic devices will be dealt with through the school complaints procedur

APPENDIX A

CODE OF CONDUCT FOR USING COMPUTERS / MOBILE DEVICES

The purpose of the Acceptable Use Agreement is to help promote a safe environment in which you can learn. The School has systems in place to monitor messages, emails and computer files and all internet activity. In using Heston's ICT systems, you agree to these simple rules.

Personal System Security

- I will only use my user name and password to log onto the School's IT Network
- I will not tell anyone my password
- I will make sure my password has characters and numbers in it
- I will change my password regularly
- I will tell my teacher if I think my password is known by somebody else

Personal Data Area

- I will only save computer files that are required for my learning
- I will organise my computer files appropriately
- I will delete any computer files I no longer need

Using Computers

- I will care for the computer / mobile devices I use and the classroom environment
- I will not print documents unnecessarily
- I will not interfere with computer cables, wires, switches or change display settings
- I will not access someone else's account without their permission
- I will not look at or delete someone else's files
- I will only use the computers / mobile devices for School purposes

Use of the Internet

- I will access the internet only to support my learning
- I understand that if I accidentally access a website that has inappropriate content, I must report it immediately to my teacher
- I will not copy or plagiarise material from the internet and, when researching, I will quote all my sources
- I will not use the School systems for accessing sites for social use e.g. Twitter, Instagram, Facebook
- I will not use the School's system to play online games
- I will not give anybody personal information e.g. my home address or telephone number or arrange to meet anyone using the internet [including friends]

Emails

- I will only send emails to people expecting to receive an email from me
- I will be polite in my emails and never make rude or personal remarks to anyone
- If I receive an email that is threatening or upsetting, I will tell my teacher
- I will only use the School email to send messages appropriate to my learning

Using the School's Network

- I will use the School's network responsibly
- I will only use appropriate language and images
- I will respect other people's privacy at all times
- I will respect other people's points of view and will be polite at all times

What can you expect?

- To be treated with respect by other students and users of IT at Heston
- The School will maintain IT systems to support your learning
- The School will work proactively to provide a safe environment in which you can use IT to support your learning
- The School will inform students of acceptable and appropriate behaviour when using IT systems
- The School will take action if the terms of the Acceptable Use Agreement are not followed

What to do if things go wrong

- If you notice something is not working or someone is not following the rules, please report what has happened to your teacher as soon as possible
- I have read and understood my responsibilities regarding the use of IT at Heston

Signed: _____

Date: _____