HUNGERHILL SCHOOL

E-SAFETY AND DIGITAL TECHNOLOGY POLICY

HUNGERHILL SCHOOL
E-SAFETY AND DIGITAL TECHNOLOGY POLICY

Rationale

1. **Rationale:**

   Digital technologies have become integral to the lives of children and young people, both within and out of school. These technologies are powerful tools, which open up new opportunities for everyone. They can stimulate discussion, promote creativity and provide a context for effective learning. Young people should have an entitlement to safe internet access at all times. It is therefore essential that, with the use of these new technologies, staff, students and parents at Hungerhill School are aware of the relative dangers and some of the legal implications of misuse.

2. **Purpose:**

   - The school e-safety policy aims to create an environment where all stakeholders including the wider school community work together to inform each other of ways to use the internet responsibly, safely and positively.
   - Students, staff and all other users of school related technologies should work together to agree a set of standards and expectations relating to appropriate usage by promoting safe and responsible access.
   - The policy is not designed to be a blacklist of prohibited activities, but instead a guide to appropriate use, leading to safer internet usage. It is intended that the positive effects of the policy will be seen on and off line; in school and at home; and ultimately beyond school and into the workplace.

3. **Roles and Responsibilities**

   The following section outlines the roles and responsibilities for all stakeholders.

   Governors, the Headteacher and the Strategic Lead for ICT will:

   - Be responsible for the approval of the e-safety Policy and for reviewing the effectiveness of the policy.

   Senior Leaders will:

   - Be responsible for ensuring including e-safety of members of Hungerhill School;
   - Be responsible for ensuring that relevant staff receive suitable training and development to enable them to carry out their e-safety roles and to train other colleagues, as relevant;
   - Ensure that there is a system in place to allow for the monitoring and support of those in the school who carry out the internal e-safety monitoring role. This is to provide a safety net and also to support key personnel who take on important monitoring roles;
   - Receive information regarding any e-safety incidents which will be logged and reviewed during SLT meetings;
   - Be aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff.

Members of SLT with responsibility for e-safety will:

- Take day to day responsibility for e-safety issues and oversee the sanctions for breaches of rules relating to e-safety;
- Ensure that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place;
- Provide training and advice to staff;
- Liaise with the Local Authority Designated Officer (LADO) or Police as appropriate;
- Liaise with and support the School's ICT technical staff;
- Ensure regular reporting of e-safety incidents to SLT as part of behaviour monitoring;
- Provide information to the Headteacher and Governors as appropriate.

4. The Strategic Lead for ICT, ICT Support Manager and ICT Technicians will:

- Ensure that the School's ICT infrastructure is secure and is not open to misuse or malicious attack and that all aspects of the School's ICT systems are secure, in line with the School's guidance and policies.
- Put in place appropriate filtering and monitoring systems, which are updated on a regular basis and keep students safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material
- Ensure that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- Conduct a full security check and monitor the school's ICT systems on a weekly basis
- Take appropriate measures to block access to potentially dangerous sites and, where possible, prevent the downloading of potentially dangerous files
- Ensure that any online safety incidents are logged and dealt with appropriately in line with this policy
- Ensure that any incidents of cyber-bullying are dealt with appropriately and in line with the school behaviour policy

All staff and volunteers will:

- Have an up to date awareness of e-safety matters and of the school's current e-safety Policy and practices;
- Have read and understood the appropriate ICT agreements;
- Ensure e-safety issues are embedded in all aspects of the curriculum and other school activities;
- Ensure students understand and follow the school's e-safety and Acceptable Use Policy;
- Ensure students have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations;
- Ensure they monitor ICT activity in lessons, extra-curricular and extended school activities;
- Ensure they are aware of e-safety issues related to the use of mobile phones, cameras and hand-held devices and that they monitor their use and implement current best practice regarding these devices;
- Ensure that in lessons where internet use is pre-planned, students should be guided to sites that are checked as suitable for their use and that processes are in place to deal with any unsuitable material that is found in internet searches.

- Report any suspected misuse or problem to a member of SLT and the ICT Support Manager;
- Ensure that digital communications with students are only on a professional level and carried out using official school systems;
- Maintain a formal and courteous and professional tone in communicating with students and ensure that professional boundaries are always maintained;
- Only use official channels of communication e.g. Office 365 and work e-mail addresses and be aware of and comply with the school's policies and guidance;
- Not exchange private text, phone numbers, personal e-mail addresses or photos of a personal nature with students;
- Firmly decline student-initiated 'friend' requests from students and not instigate any. Use discretion when dealing with friend requests from parents. It is acceptable to decline these invitations and remind parents of more formal channels which they can discuss their child's education;
- Operate online in a way which would not call into question their position as a professional;
- Manage privacy settings and keep them under review. These are particularly important regarding photos, and remember that no privacy mechanism is 100% guaranteed;
- Ensure settings prohibit others from tagging them in any photos or updates without explicit permission. Staff must always ask others to remove any undesirable content related to them;
- Be aware that potential employers may try and view your online social media profiles;
- Consider that conversations held online may not be private. Be aware of who may have access to what is posted;
- Assume that information posted can be accessed and altered;
- Not discuss students, colleagues, parents or carers online or criticise your employer or others within the school community;
- Respect student privacy and confidentiality always;
- Use strong passwords and change them regularly. Protect mobile phones smart phones/tablet computers with a PIN, especially when in school to protect access to its content and potential misuse;
- Bring the matter to the attention of the Headteacher using the proper procedures, if they are the victim of cyber bullying or are uncomfortable with comments, photos or posts made by students in relation to them.
- Audit and re-evaluate the information about them and who has access to it if they are entering a programme of teacher education, or Teacher Induction Period.

It is understood that social media can play an important part in communication between the School and students, parents/carers; however, there is also a need to ensure it is used in an appropriate and safe way. Before any member of staff sets up a resource such as a student blog space or a school Twitter account, they must seek permission from the Headteacher and they should ensure that appropriate steps are taken to make such social media 'private' so that only people they approve can access it. The member of staff will then be responsible for the posts made on the site and for moderating the content from other users/contributors;

The School uses a filtered service and will endeavour to ensure that inappropriate material is not accessible by students. However, any staff with knowledge of

inappropriate sites available through the filtered access should inform the ICT Support Manager as a matter of urgency.

Before posting materials online, staff should stop and ask themselves:

- Might it reflect poorly on them, the school, employer or the teaching profession?
- Is their intention to post this material driven by personal reasons or professional reasons?
- Are they confident that the comment or other media in question, if accessed by others, (colleagues, parents etc.) would be considered reasonable and appropriate?"

Designated Safeguarding Leads

Should be trained in e-safety issues and be aware of the potential for serious child protection issues to arise from:

- Sharing of personal data;
- Access to illegal/inappropriate materials;
- Inappropriate on-line contact with adults/strangers;
- Potential or actual incidents of grooming;
- Cyber-bullying

Students will ensure that:

- They are responsible for using the School's ICT systems in accordance with school policy, which they will be expected to sign for before being given access to the school's systems (Appendix 1);
- They have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations;
- They need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so;
- They should understand the importance of adopting good e-safety practice when using digital technologies out of school and realise that the school's E-Safety Policy covers their actions out of school, if related to their membership of the school.
- They are responsible for ensuring digital devices, including mobile phones, are only used with the permission of the teacher. Mobile phones should be switched off and kept in bags throughout the school day including before school, break, lunchtimes and movement times. They should not be used until leaving the site at the end of the school day.

Students must ensure that files stored on their digital devices/phones do not contain inappropriate images e.g. violent, degrading or offensive. The transmission of some images/information can be a criminal offence and will be dealt with as such by the school.

Responsibility for the digital device/phone rests solely with the student and the school accepts no financial responsibility for damage, loss, theft or costs incurred when using the phone for any purpose.

Individual users of the Internet are responsible for their behaviour and communications over the network. Users will comply with school standards and will honour the agreements they have signed.

Users should expect that electronic communications, files stored on servers or other storage media will be open to inspection.

During school, teachers will guide students toward appropriate materials. Outside of school, families bear responsibility for such guidance and they must also exercise with care, information sources such as television, telephones, movies, radio and other potentially offensive media

Parents/Carers

Parents/carers play a crucial role in ensuring that their children understand the need to use the internet/mobile devices in an appropriate way.

Parents and carers will be responsible for:

- Endorsing the school's E-Safety Policy;
- Accessing the school website in accordance with the relevant Acceptable Use Policy.
- Informing the school of any concerns arising from the inappropriate use of digital media and the internet.

Education and Training - Students

E-Safety education will be provided in the following ways:

- A planned e-safety programme will be provided as part of the ICT curriculum;
- Key e-safety messages will be reinforced as part of a planned programme of assemblies and within the PSHE curriculum;
- Students will be taught, whenever an opportunity occurs. to be critically aware of the material/content they access on-line and be guided to validate the accuracy of information;
- Students will be encouraged to adopt safe and responsible use of ICT, the internet and mobile devices both within and outside the school;
- Students will be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet;

Education and Training – Staff

It is essential that all staff receive e-safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- E-safety training for all staff is included as part of Level 1 child safeguarding training;
- All new staff will receive e-safety training as part of their induction programme, ensuring they understand the E-safety Policy and Acceptable Use Policy.

Training – Governors

Governors are required to undertake the School's e-safety training as part of regular, scheduled, safeguarding training.

Infrastructure, equipment, filtering and monitoring

Both the Strategic Lead for ICT and the ICT Support Manager will be responsible for ensuring that the School's infrastructure/network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented.

- All users will have clearly defined access rights to School's ICT systems;
- All users will be provided with a username and password by ICT support who will keep an up to date record of users and their usernames. Users will be required to change their password regularly;
- Users will be made responsible for the security of their username and password, must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security;
- In the event of the ICT Support Manager (or other member of the IT Support Team) needing to switch off the filtering for any reason, or for any user, this must be logged and carried out by a process that is agreed by the Headteacher;
- Requests from staff for sites to be removed from the filtered list will be considered by the ICT Support Manager;
- ICT technical staff regularly monitor and record the activity of users on the School's ICT systems and users are made aware of this in the Acceptable Use Policy;
- Remote management tools are used by staff to control workstations and view users' activity;
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, hand held devices etc from accidental or malicious attempts which might threaten the security of the School's systems and data;
- Guest users may be granted a temporary log in or guest account if agreed by the ICT Support Manager;
- Personal use of the School's ICT systems should be limited to what may be deemed reasonable. The services are provided predominantly for education purposes;
- Neither staff nor students should install programmes or other software on workstations, portable devices or servers, without the prior express, written permission of the School's ICT Support Manager;
- The School's ICT infrastructure and individual workstations are protected by up to date virus software;
- Personal data (as defined by the Data Protection Act 2018) must not be sent over the internet or taken off school premises unless safely encrypted or otherwise secured by password or other means;

Use of digital and video images - Photographic, Video

The development of digital imaging technologies has created significant benefits to learning, allowing staff and students instant use of images that they have recorded themselves or downloaded from the internet. However, staff and students need to be aware of the risks associated with sharing images and with posting digital images on the internet. Those images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. This information will be reviewed and updated on an annual basis to ensure that the information remains current.

The following procedures must always be observed:

- When using digital images, staff should inform and educate students about the risks associated with the taking, use, sharing, publication and distribution of images. They should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites;
- Staff can take digital / video images to support educational aims, but must follow School policies concerning the sharing, distribution and publication of those images. Those images should only be taken using School equipment; the personal equipment of staff should not be used for such purposes. They should also only be stored on the School's network and not on any personal device;
- Care should be taken when taking digital/video images that students are appropriately dressed and are not participating in activities that might bring the individuals or the School into disrepute;
- Students must not take, use, share, publish or distribute images of others without their permission;
- Photographs published on the website, or elsewhere that include students will be selected carefully and will comply with good practice guidance on the use of such images;
- Written permission from parents or carers will be obtained before photographs of students are published on the School website (this is covered as part of the agreement signed by parents or carers);
- Be aware that downloading, copying or printing images from the internet may also breach copyright laws.

Data Protection and GDPR

The Data Protection Act 2018 and the GDPR legislation effective from 25th May 2018 states that personal data must be:

- processed lawfully, fairly and in a transparent manner in relation to individuals ('lawfulness, fairness and transparency');
- collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be incompatible with the initial purposes ('purpose limitation');
- adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');
- accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy');
- kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals ('storage limitation');
- processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality').

Staff must ensure that they:

- Take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse;
- Use personal data only on secure password protected computers and other devices, ensuring that they are properly 'logged-off' at the end of any session in which they are using personal data;
- Transfer data using appropriately encrypted and secure means.

When personal data is stored on any portable computer system, USB stick or any other removable media:

- the data must be encrypted, and password protected;
- the device must be password protected (many memory sticks / cards and other mobile devices cannot be password protected, if this is the case then each individual file will need to be password protected);
- the data must be securely deleted from the device, once it is no longer required.

Unsuitable / inappropriate activities

Some internet activity e.g. accessing child abuse images or distributing racist material is illegal and is obviously be banned from the School and all other ICT systems. Other activities e.g. Cyber-bullying, use of electronic communications to radicalise children or others, is banned and could lead to criminal prosecution. There are however a range of activities which may, generally, be legal but would be inappropriate in a school context, either because of the age of the users or the nature of those activities.

Responding to incidents of misuse

It is hoped that all members of the School community will be responsible users of ICT, who understand and follow this policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse. Listed below are the responses that will be made to any apparent or actual incidents of misuse and must be reported immediately to the Headteacher. The Headteacher must be informed immediately. The Headteacher and any other relevant members of the SLT must inform the relevant authorities immediately of any concerns/ infringements. The steps taken must all be reported to the Governing Body.

Guidance

The following are deemed inappropriate and staff should record and report any of these behaviours

- Illegal activities of any kind
- Bypassing the school's filtering system
- Viewing pornographic material
- Using social media or email in lesson time without the permission of the teacher
- Cyber bullying

- Writing malicious comments about the school or bringing the school name into disrepute whether in school time or not
- Sharing usernames and passwords
- Deleting someone else's work or unauthorized deletion of school files
- Trying to hack or hacking into another person's account, school databases, school website, school emails or online fraud
- Uploading or downloading inappropriate material using the school network
- Copyright infringement of text, software or media
- Using a mobile phone or other digital device in a lesson without permission
- Listening to music through personalised media during school time. This includes lessons, breaks and lunchtime.
- Using a phone/digital device to broadcast music or transfer inappropriate material.
- Using a mobile phone or digital device to photograph/video students or staff without the consent of the person being photographed.
- Wearing earphones during or between lessons, for reasons of health and safety and courtesy
- Taking a phone/digital device into an examination room

Sanctions will be applied for a breach of any of the above

- Parents will be informed of any breach of guidelines**.**
- Violations of the above rules will result in a temporary or permanent ban of Internet use.
- Additional disciplinary action may be added in line with existing school policy.
- When applicable, the police or local authorities will be involved.

Sanctions will be applied for a breach of any of the above

- If a student uses a mobile phone/digital device without permission on school property, it will be confiscated and taken to reception for safe storage. The student will be issued with a detention of sixty minutes after school via the student planner. It is the student's responsibility to inform their parent/guardian of the detention. The student can collect their mobile phone/digital device from reception at the end of the day.
- If a mobile phone/electronic device is confiscated for a second time in one term, it will be taken to reception. The student will be issued with a Friday, SLT detention of ninety minutes after school, 3:10 pm to 4:40 pm. It is the student's responsibility to inform their parent/guardian of the detention. The student can collect their mobile phone/digital device from reception at the end of the day.
- If a mobile phone/electronic device is confiscated for a third time in one term, sanctions such as isolation and loss of social time will be applied. In addition, the parent/guardian will be invited into school for a meeting with the achievement leader/leadership team to agree the way forward.

Appendix 1

Acceptable Usage agreement for students and parents

This is the acceptable usage agreement for our school. The purpose of this agreement is to promote positive and responsible network and Internet use. Please read carefully and sign at the bottom to show you agree to these terms. If you do not sign and return this form you will not be able to use the school's IT systems.

For students:

- I will only use school Internet and IT facilities for educational purposes which follow the teachers' instructions. This includes email, video, messaging, video-conferencing, social media, Internet, file-saving and printing.
- I will not use my mobile phone during lessons, tutor group time, clubs or other activities organised by the school, without a teacher's permission. If permission is granted, I will use it responsibly, and will not access any inappropriate websites or other inappropriate material or use inappropriate language when communicating online. I will use my mobile device as if it was a school computer, following all the rules for using school computers.
- I will not install software on school IT facilities due to the risk of damage being caused by malware or viruses. I will ask an ICT teacher to install software if required.
- I will not share my network, Internet or any other school-related passwords.
- I will change my passwords when asked to.
- I will only use my school-supplied email address for school-related activities.
- I will not look at or delete other people's work or files.
- I will make sure all my contact with other people at school is responsible. I will not cyber-bully students or teachers.
- I will be responsible and polite when I talk online to students, teachers and other people related to the school, both in school time and outside school-time.
- I will not look for or look at inappropriate websites in school. I will check with a teacher if I think a website might be unsuitable.
- I will not use chat rooms
- I will not give out my personal details, such as my name, address, school or phone number on the Internet.
- I will not meet people I've met on the Internet unless I have told my parents and they come with me.
- I will not open any attachments in emails, or follow any links in emails, without first checking with a teacher
- I will not upload or download any pictures, writing or films which might upset people online.
- I will not use any inappropriate language when communicating online, including in emails
- I will not write inappropriate or untrue comments online about students, teachers or the school.
- I will treat all IT equipment at school with respect and ensure the computer is left in the state that I found it.
- I am aware that everything I do on the computers at school is monitored and logged, and that the school can talk to my parents if a teacher is concerned about my online safety or my behaviour when using school computers.
- I will respect copyright when making use of images and videos in my school work. I will acknowledge sources used.

- I will not look for, view, upload or download offensive, illegal, copyright-infringing or pornographic material. If I find such material on school IT equipment I will inform a teacher immediately.
- Images of students will only be taken, stored and used for school purposes in line with school policy. Images will only be used on the Internet or in the media with permission.
- I will not look for ways to bypass the school filtering or proxy service.
- I will not bypass the school filtering or proxy service.
- I understand that these rules are designed to keep me safe and that if they are not followed, sanctions may be applied and my parent/guardian may be contacted.

The following sanctions can be applied:

- Physical damage to equipment – Parents will be asked to reimburse the school.
- Abuse of email system, including sending of abusive or threatening messages will lead to the removal of email access for at least half a term. School will encourage the family of the victim/s to involve the police, who may prosecute.
- Repeat offences – will lead to the permanent removal of network access
- Abuse of the internet, including accessing or attempting to access inappropriate material will lead to the temporary removal of internet access.
- Serious abuse of the rules around Network use may also result in further punishment under the school Code of Discipline
- The school reserves the right to vary the sanction if access to the system is required for compulsory study.

I accept to be bound by the Hungerhill School Computer Network & Electronic Resources Acceptable Use agreement.

Name…… Form……..

Signed……..……(Student)

Date…….

For parents/carers:

Every effort is made to ensure a safe environment for our students; however, it is not possible to filter every web site that may be inappropriate or block individual videos on sites such as YouTube. We believe that the benefits to students in the form of information resources and opportunities for collaboration exceed the disadvantages; however, we regard the use of ICT equipment as a privilege which will be removed if a student is found to have acted inappropriately.

I agree that my child can use the school's ICT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for students using the school's ICT systems and internet, and for using personal electronic devices in school, and will make sure my child understands these. I am happy for my son/daughter to have full access to the internet including YouTube and accept that while every effort is made to ensure a safe environment, it is not possible to filter every web site that may be inappropriate. I give my child permission to have access to the school email system and to be provided with a school email address when required to support their study.

Signed:…….Parent/Carer:

Date ……..

Appendix 2

Acceptable Usage agreement:

Staff, support staff, governors, visitors, wider stakeholders with access and external contractors

When using the school's ICT systems and accessing the internet in school, or outside school on a work device:

- I will not access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or pornographic nature
- I will not use them in any way which could harm the school's reputation
- I will not access social networking sites or chat rooms
- I will not use any improper language when communicating online, including in emails or other messaging services
- I will only use school IT systems, external logins and email for school related purposes. Other use will be with the permission of the SLT.
- I will not divulge any school related passwords and I will comply with school IT security procedures.
- I will make sure email and social media interactions with staff, parents, students and members of the public are responsible and in line with school policies and DfE/GTC/TA guidelines.
- I will not give my home address, phone number, mobile number, personal social networking details or email address to students.
- I accept that students may find these details out, and that any contact should be logged and either not reciprocated or replied to in line with school policies.
- I should be responsible and aware of my professional responsibilities and school policies if I supply any personal details to parents.
- I will use school email systems for school related communications.
- I will not use personal accounts for school business.
- I will ensure that personal data is stored securely and in line with the Data Protection Act.
- I will follow school policy regarding external logins, encrypted data and not storing school material on personal IT equipment.
- I will not install software onto workstations or the network unless supervised by the Network Manager or IT support staff.
- I will not search for, view, download, upload or transmit any material which could be considered illegal, offensive, defamatory or copyright infringing.
- Photographs of staff, students and any other members of the school community will not be used outside of the internal school IT Network unless written permission has been granted by the subject of the photograph or their parent/guardian.
- I will ask the permission of the Head Teacher (on site) or the proprietor of the building (off site) prior to taking any photographs.
- I am aware that all network and internet activity is logged and monitored and that the logs are available to SLT in the event of allegations of misconduct.
- I will not write or upload any defamatory, objectionable, copyright infringing or private material, including images and videos, of students, parents or staff on social media or websites in any way which might bring the school into disrepute.

- I will make sure that my internet presence does not bring the teaching profession into disrepute and that I behave online in line with DfE and TA guidelines.
- I will take all reasonable steps to ensure that work devices are secure and password-protected when using them outside school, and keep all data securely stored in accordance with this policy and the school's data protection policy.
- I will let the designated safeguarding lead (DSL) and ICT manager know if a student informs me they have found any material which might upset, distress or harm them or others, and will also do so if I encounter any such material.
- I will champion the school's E-Safety policy and be a role model for positive and responsible behaviour on the school network and the Internet.

Signed: …….

Date: ……..