A WHOLE SCHOOL POLICY FOR

E-SAFETY AND ICT ACCEPTABLE USE

INTRODUCTION

The Heathland School recognises the benefits that can be made to education through the use of Information and Communication Technology (ICT). Advances in ICT have brought about fresh challenges enabling us to learn in new and exciting ways. ICT offers us a means of carrying out tasks to a higher standard more efficiently and, in education, raising standards and streamlining educational administration.

E-Safety encompasses internet technologies and electronic communications such as mobile telephones and wireless technology. Use of the school's ICT equipment by any members of the school community must be in accordance with this policy. Any use which infringes this policy will be treated very seriously by the School Governing Body.

This policy applies to all members of the school community (including staff, pupils, governors, volunteers, parents/guardians and visitors) who have access to and are users of school IT systems, both in and out of school. The school will deal with cyber-bullying or other e-safety incidents covered within this policy and associated behaviour and anti-bullying policies and will inform parents/guardians of incidents of inappropriate e-safety behaviour that take place in or out of school.

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 management information 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.

LEADERSHIP AND MANAGEMENT

Governors are responsible for the approval of the e-safety policy and for reviewing the effectiveness of the policy through the Governors' Pupils Committee. The day to day responsibility for e-safety lies with the Deputy Head (Pupil Support).

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 Head (Resources and Community) for investigation/action/sanction.

RESPONSIBILITIES

New technologies have become integral to the lives of children and young people in today's society, both within educational establishments and in their lives outside school. However, the use of these new technologies can put young people at risk within and outside the school. Some of the dangers they may face include:

- Access to illegal, harmful or inappropriate images or other content.
- Unauthorised access to, loss of or sharing of personal information.
- The risk of being subject to grooming by those with whom they make contact on the Internet.
- The sharing/distribution of personal images without an individual's consent or knowledge.
- Inappropriate communication/contact with others, including strangers.
- Cyber-bullying.
- Access to unsuitable video/Internet games.
- An inability to evaluate the quality, accuracy and relevance of information on the Internet.
- Plagiarism and copyright infringement.
- Illegal downloading of music or video files.
- The potential for excessive use which may impact on the social and emotional development and learning of the young person.

Many of these risks reflect situations in the off-line world and it is essential that this e-safety policy is read and used in conjunction with other school policies; specifically Anti-Bullying, Pupil Behaviour and Child Protection.

As with all other risks, it is impossible to eliminate those risks completely. It is therefore essential, through good educational provision, to build pupils' resilience to the risks to which they may be exposed so that they have the confidence and skills to face and deal with these risks.

Teaching & Support Staff

In addition to elements covered in the Staff Accessible Usage Policy (AUP), all teaching and support staff are responsible for ensuring that:

- They have an up to date awareness of e-safety matters and of the current school e-safety policy and practices

- They have read, understood and signed the school Staff Acceptable Usage Policy (AUP)

- E-safety issues are embedded in all aspects of the curriculum and other school activities

- Students understand and follow the school's e-safety and acceptable usage policies

- Students have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations

- They monitor ICT activity in lessons and extra-curricular activities

- In lessons where Internet use is pre-planned, pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in Internet searches.

Pupils

- Are responsible for using the school ICT systems in accordance with the Pupil Acceptable Usage Policy, which they will be required to sign before being given access to school systems. Parents/guardians will be required to read through and sign alongside their child's signature.

- Need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so.

- 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 also covers their actions out of school, if related to their membership of the school.

Parents/Guardians

Parents/guardians play a crucial role in ensuring that their children understand the need to use the Internet/mobile devices in an appropriate way. Research shows that many parents and carers do not fully understand the issues and are less experienced in the use of ICT than their children. The school will therefore take opportunities to help parents understand these issues. Parents and guardians will be responsible for:

- Endorsing (by signature) the Pupil Acceptable Usage Policy.

- Accessing the school website in accordance with the relevant school Acceptable Usage Policy.

MANAGEMENT OF INTERNET ACCESS

- The school ICT system capacity and security will be reviewed regularly.
- Virus protection will be installed and updated regularly.

E mail

- Pupils may only use approved e-mail accounts on the school system.
- Pupils must immediately inform a member of staff if they receive an offensive e-mail.
- Pupils must not reveal any details of themselves or others such as address or telephone number, or arrange to meet anyone in any e-mail communication without specific permission.
- Incoming e-mail should be treated as suspicious and attachments not opened unless the author is known.
- E-mails sent to external organisations should be written carefully and authorised before sending in the same way as a letter written on school headed paper.
- Pupils should use the school e-mail system for work and educational purposes and NOT for personal chat or for social networking.
- When communicating with pupils and parents, staff should only use their school e-mail account.
- When teaching a lesson, teachers should only use e-mail for safeguarding purposes.

Digital Images

- The school record of parental permissions granted/not granted must be adhered to when taking images of our pupils.
- Under no circumstances should images be taken using privately owned equipment without the express permission of the Head teacher or the Network Manager.
- Where permission is granted the images should be transferred to school storage systems and deleted from privately owned equipment at the earliest opportunity.
- Permission to use images of all staff who work at the school is sought on induction and a copy is located in the personnel file.

Social networking and personal publishing

- The school will block access to social networking sites.
- Newsgroups will not be made available to pupils unless an educational requirement for their use has been demonstrated.
- Pupils will be advised never to give out personal details of any kind which may identify them or their location.

- Staff and pupils must not place personal photos on any social network space without considering how the photo could be used now or in the future.

- Staff should be aware of the potential risk to their professional reputation by adding pupils, parents or friends of pupils as 'friends' on their social network site and are strongly recommended not to do so.

- If inappropriate comments are placed on social networking sites about the school or school staff then advice would be sought from the relevant agencies, including the police if necessary.

- Pupils will be taught about e-safety on social networking sites as we accept some may use it outside of school.

Although many of the above points are preventative and safeguarding measures, it should be noted that the school will endeavour whenever possible to use social networking in positive ways to publicise, inform and communicate information. The school has active website and twitter accounts which are used to inform, publicise school events and celebrate and share the achievement of students.

Websites

- In lessons where Internet use is pre-planned, pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in Internet searches.

- Staff will preview any recommended sites before use.

- "Open" searches (e.g. "find images/ information on...") are discouraged when working with younger pupils who may misinterpret information.

- If Internet research is set for homework, specific sites will be suggested that have previously been checked by staff.

- **All** users must observe copyright of materials published on the Internet.

- Staff setting an internet task will regularly check what is being viewed by the pupils. Pupils are also aware that all internet use at school is tracked and logged.

- The school only allows the Network Manager and the Senior Management Team to access internet logs.

Copyright

- Pupils will be taught an appropriate understanding of research skills and the need to avoid plagiarism and uphold copyright regulations and staff will monitor this.

- Pupils are taught, appropriate to their age, to acknowledge the source of information used and to respect copyright when using material accessed on the Internet.

- If using a search engine for images staff and pupils should open the selected image and go to it's website to check for copyright.

Managing Filtering

- The school will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

- If staff or pupils discover unsuitable sites, the URL address and content must be reported to the Network Manager.

Use of Own Equipment

- Privately owned ICT equipment should never be connected to the school's network without the specific permission of the Head teacher or Network Manager.

- Pupils should not bring their own removable data storage devices into school.

- Pupils should not bring in their own equipment unless asked to do so by a member of staff.

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 Ctrl, Alt, Del 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 3 months.

- Users should not use the same password on multiple systems or attempt to "synchronise" passwords across systems

- Pupils should only let school staff know their in-school passwords.

- Pupils must inform staff immediately if passwords are traced or forgotten. Pupils must see a member of the Network Team to have their password reset.

EDUCATION AND TRAINING

PUPILS

- E-safety education is provided as part of PSHE and is regularly revisited in Information Technology and other lessons across the curriculum.

- Pupils 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.

- Pupils are helped to understand the need for the Pupil AUP and encouraged to adopt safe and responsible use of ICT, the Internet and mobile devices both within and outside of school.

- Pupils 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 posted in school.

- Staff act as good role models in their use of ICT, the Internet and mobile devices.

STAFF

- The Deputy Head (Pupil Support) 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 E-Safety policy, Acceptable Usage 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 their line manager or the Deputy Head (Resources & Community).

MONITORING

All use of the school's Internet access is logged and the logs are randomly but regularly monitored by the school's external provider. Whenever any inappropriate use is detected it will be followed up by the Deputy Head (Pupil Support).

Any e-safety incidents must immediately be reported to the Head teacher (if a member of staff) or the Deputy Head (Pupil Support) (if a pupil) who will investigate further following e-safety and safeguarding policies and guidance.

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 in Appendix 2 are the responses that will be made to any apparent or actual incidents of misuse. It is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the school community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal behaviour/disciplinary procedures (Appendix 3).

REVIEW AND EVALUATION

The E-Safety and ICT Acceptable Use Policy will be reviewed annually

June 2019

APPENDIX 1

Communications

A wide range of rapidly developing communications technologies has the potential to enhance learning. The following table shows how the school currently considers the benefit of using these technologies for education outweighs their risks/disadvantages:

		Staff and other adults			Students and young people			
Communication Technologies		Permitted	Permitted at certain times	Not Permitted	Permitted	Permitted at certain times	Allowed with staff permission	Not Permitted
Mobile phones May be brought to school		✓						✓
Mobile phones used in lessons				✓				✓
Use of mobile phones in social time		✓						✓
Taking photographs on mobile devices			✓					✓
Use of tablets and other educational mobile devices		✓						✓
Use of school email for personal emails				✓				✓
Social use of chat rooms/facilities				✓				✓
Use of social network sites for educational purposes		✓					✓	
Use of educational blogs		✓			✓			

When using communication technologies the school considers the following as good practice:

- The official school email service may be regarded as safe and secure and is monitored. Staff and students should therefore use only the school email service to communicate with others when in school, or on school systems (e.g. by remote access).
- Users need to be aware that email communications may be monitored
- Users must immediately report, to the nominated person (in accordance with the school policy) the receipt of any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature and must not respond to any such email.
- Any digital communication between staff and pupils or parents/carers (email, chat, Learning Platform etc) must be professional in tone and content. These communications may only take place on official (monitored) school systems. Personal email addresses, text messaging or public chat/social networking programmes must not be used for these communications.
- Students should be taught about email safety issues, such as the risks attached to the use of personal details. They should also be taught strategies to deal with inappropriate emails and be reminded of the need to write emails clearly and correctly and not include any unsuitable or abusive material.
- Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff.

APPENDIX 2

Unsuitable / inappropriate activities

The school believes that the activities referred to in the following section would be inappropriate in a school context and that users, as defined below, should not engage in these activities in school or outside school when using school equipment or systems. The school policy restricts certain internet usage such that users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:

User actions	Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Child sexual abuse images					✓
Promotion or conduct of illegal acts, eg under the child protection, obscenity, computer misuse and fraud legislation					✓
Adult material that potentially breaches the Obscene Publications Act in the UK					✓
Criminally racist material in the UK					✓
Pornography					✓
Promotion of any kind of discrimination				✓	
Promotion of racial or religious hatred					✓
Threatening behaviour, including promotion of physical violence or mental harm					✓
Any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute				✓	
Using school systems to run a private business				✓	
Use systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school				✓	
Uploading, downloading or transmitting commercial software or any copyrighted materials belonging to third parties, without the necessary licensing permissions				✓	
Revealing or publicising confidential or proprietary information (eg financial / personal information, databases, computer / network access codes and passwords)				✓	
Creating or propagating computer viruses or other harmful files				✓	
Carrying out sustained or instantaneous high volume network traffic (downloading / uploading files) that causes network congestion and hinders others in their use of the internet				✓	
On-line gaming (educational)		✓			
On-line gaming (non- educational)/gambling				✓	
On-line shopping / commerce			✓		
File sharing			✓		
Use of social networking sites			✓		
Downloading video broadcasting eg Youtube	✓				
Uploading to video broadcast eg. Youtube			✓		

APPENDIX 3

The guidance in this policy should be implemented with cross reference to the School's Child Protection, Anti-Bullying and Behaviour Policies. Note, attempts have been made to synchronise guidance and sanctions.

Incident involving students	**Teacher to use school behaviour policy to deal with**	**Refer to Head of Year/Deputy Head (Pupil Support)**	**Refer to police**	**Refer to Network Manager for action re security/filtering etc**
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable/ inappropriate activities**).**		✓	✓	✓
Unauthorised use of non-educational sites during lessons	✓			✓
Unauthorised use of mobile phone/ digital camera/ other handheld device.		✓		
Unauthorised use of social networking/ instant messaging/ personal email	✓	✓		✓
Unauthorised downloading or uploading of files		✓		✓
Allowing others to access school network by sharing username and passwords		✓		✓
Attempting to access or accessing the school network, using another student's account		✓		✓
Attempting to access or accessing the school network, using the account of a member of staff		✓		✓
Corrupting or destroying the data of other users		✓		✓
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature		✓		✓
Continued infringements of the above, following previous warnings or sanctions		✓	Community Police Officer referral	✓
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school		✓		✓
Using proxy sites or other means to subvert the school's filtering system		✓		✓
Accidentally accessing offensive or pornographic material and failing to report the incident		✓		✓

THE HEATHLAND SCHOOL **APPENDIX 4**

ICT ACCEPTABLE USAGE POLICY

for staff, governors, visitors, and wider stakeholders with access to the school's network.

- I will only use school IT systems, external logins and email for school related purposes. Other use will be with the permission of a member of SMT.
- I will not use my personal email accounts or social media accounts or related sites for work purposes at any time
- 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, pupils and members of the public are responsible and in line with school policies.
- I will not give my home address, phone number, mobile number, personal social networking details or personal email address to pupils. I accept that pupils may find these details out, and that any contact should be logged and not reciprocated. 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 General Data Protection Regulation. I will follow school policy with regard to external logins, encrypted data and not storing school material on personal IT equipment. I will report any issues related to breaches to the Data Protection Officer immediately – Deputy Head [Resources and Community].
- 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, pupils 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 am aware that all network and internet activity, including personal e mails, is logged and monitored and that the logs are available to SMT in the event of allegations of misconduct.
- If I purchase personal items through the school system I do so at my own risk.
- I will not write or upload any defamatory, objectionable, copyright infringing or private material, including images and videos, of pupils, 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 guidelines.

- I will champion the school's E-Safety policy and be a role model for positive and responsible behaviour on the school network and internet.
- I will ensure my computer is locked if I leave it unattended in a classroom.
- I will not use e-mail during a lesson unless there is a safeguarding issue
- I will ensure any electronic personal data is used and stored in accordance with the school's GDPR guidance

FAILURE TO ADHERE TO THE ICT ACCEPTABLE USAGE POLICY MAY LEAD TO DISCIPLINARY ACTION.

THE HEATHLAND SCHOOL

ICT ACCEPTABLE USAGE POLICY

NAME (please print) : _____

I HAVE READ AND UNDERSTOOD THE ICT ACCEPTABLE USAGE POLICY AND AGREE TO ABIDE BY THE TERMS AND CONDITIONS THEREIN.

SIGNED : _____ DATE :_____

ICT ACCEPTABLE USAGE POLICY

Appendix 5

Our policy is to promote positive and responsible network and internet behaviour. 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 schools' IT systems.

- I will only use school internet and IT facilities for educational purposes which follow the teachers' instructions.
- I will not use the school IT facilities to play games unless otherwise instructed by a teacher.
- I will not install software or look for ways to bypass the school filtering proxy service.
- I will not share my network, internet or any other school-related email/passwords.
- 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 always be responsible and polite when I talk online to pupils, teachers and other people related to the school.
- I won't give out my personal details, such as my name, address, school or phone number on the internet.
- I won't meet people I've met on the internet unless I have told my parents and they come with me.
- I won't write unpleasant, rude or untrue comments online about pupils, 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.
- I will be responsible and respect copyright when making use of images and videos in my school work.
- 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.

I understand that these rules are designed to keep me safe and if they are not followed, sanctions may be applied and my parent/guardian will be contacted. I have read and understood these rules and abide by them.

Pupils Name: _____ Signature: _____

Tutor Group_____

Parent/Guardians Signature: _____