HLTY E-SAFETY POLICY and ACCEPTABLE USE AGREEMENT for STUDENTS

THIS POLICY APPLIES TO THE HOPE TRUST BOARD, ALL TRUST SCHOOLS AND THE HOPE TEACHER TRAINING PARTNERSHIP

Document Management:

Date Policy Approved: 09 April 2018
Date Amended: July 2019
Next Review Date: July 2020
Version: 1.1
Approving Body: Resources Committee

Contents

Statement of intent

At **Hope Learning Trust, York (HLTY)**, we understand that computer technology is an essential resource for supporting teaching and learning. The internet, and other digital and information technologies, open up opportunities for students and play an important role in their everyday lives.

Whilst the Trust recognises the importance of promoting the use of computer technology throughout the curriculum, we also understand the need for safe internet access and appropriate use.

The Trust has created this policy with the aim of ensuring appropriate and safe use of the internet and other digital technology devices by all students and staff.

The Trust is committed to providing a safe learning and teaching environment for all students and staff, and has implemented important controls to prevent any harmful risks.

The purpose of this policy is to:

- set out the key principles expected of all members of the HLTY community with respect to the use of IT-based technologies.
- safeguard and protect the children of the Trust.
- assist HLTY staff working with children to work safely and responsibly with the Internet and other communication technologies and to monitor their own standards and practice.
- set clear expectations of behaviour and/or codes of practice relevant to responsible use of the Internet for educational, personal or recreational use.
- have clear structures to deal with online abuse such as online bullying which are cross referenced with other Trust policies.
- ensure that all members of the HLTY community are aware that unlawful or unsafe behaviour is unacceptable and that, where appropriate, disciplinary or legal action will be taken.
- minimise the risk of misplaced or malicious allegations made against adults who work with students.

Signed by:

_____	Headteacher/Principal	Date:	_____
_____	Chair of Resources Committee	Date:	_____

1. Legal framework

1.1. This policy has due regard to the following legislation, including, but not limited to:

- Human Rights Act 1998
- GDPR 2018
- Freedom of Information Act 2000
- Regulation of Investigatory Powers Act 2000
- Safeguarding Vulnerable Groups Act 2006
- Education and Inspections Act 2006
- Computer Misuse Act 1990, amended by the Police and Justice Act 2006
- Communications Act 2003
- Protection of Children Act 1978
- Protection from Harassment Act 1997

1.2. This policy also has regard to the following statutory guidance:

- DfE (2016) 'Keeping children safe in education'

1.3. This policy will be used in conjunction with the following school policies and procedures:

- E-security Policy
- Cyber Bullying Policy
- Social Media Policy
- Allegations of Abuse Against Staff Policy
- Acceptable Use Agreement - Students (**APPENDIX A**)

2. Roles and responsibilities

- It is the responsibility of all staff to be alert to possible harm to students or staff due to inappropriate internet access or use, both inside and outside of the school, and to deal with incidents of such as a priority.
- The Local Governing Committee (LGC) is responsible for ensuring that there are appropriate filtering and monitoring systems in place to safeguard students.
- The **e-Safety Officer**, **named at each school in APPENDIX B**, is responsible for ensuring the day-to-day e-Safety in the school, and managing any issues that may arise.
- The **e-Safety Officer** is responsible for chairing the **e-Safety committee**, which includes representatives of the school **senior leadership team (SLT)**, teaching staff, governors, parents, students and wider school community.

- The **Headteacher/Principal** is responsible for ensuring that the **e-Safety Officer** and any other relevant staff receive CPD to allow them to fulfil their role and train other members of staff.
- The **e-Safety Officer** will provide all relevant training and advice for members of staff as part of the requirement for staff to undergo regularly updated safeguarding training and be able to teach students about online safety.
- The **Headteacher/Principal** will ensure there is a system in place which monitors and supports the **e-Safety Officer**, whose role is to carry out the monitoring of e-Safety in the school, keeping in mind data protection requirements.
- The **e-Safety Officer** will regularly monitor the provision of e-Safety in the school and will provide feedback to the **Headteacher/Principal**.
- The **e-Safety Officer** will maintain a log of submitted e-Safety reports and incidents.
- The **Headteacher/Principal** will establish a procedure for reporting incidents and inappropriate internet use, either by students or staff.
- Cyber bullying incidents will be reported in accordance with the school's **Anti-Bullying and Harassment Policy**.
- LGCs will hold regular meetings with the **e-Safety Officer** to discuss the effectiveness of the e-Safety provision, current issues, and to review incident logs, as part of the school's duty of care.
- The LGCs will evaluate and review this E-Safety Policy on a **termly** basis, taking into account the latest developments in ICT and the feedback from staff/students.
- The **Headteacher/Principal** will review and amend this policy with the **e-Safety Officer**, taking into account new legislation, government guidance and previously reported incidents, to improve procedures.
- All staff and students will ensure they understand and adhere to our **Acceptable Use Agreement**, which they must sign and return to the **Headteacher/Principal**.
- Parents are responsible for ensuring their child understands how to use computer technology and other digital devices appropriately.
- The **Headteacher/Principal** is responsible for communicating with parents regularly and updating them on current e-Safety issues and control measures.
- All students are aware of their responsibilities regarding the use of school-based ICT systems and equipment, including their expected behaviour.

3. Use of the internet

3.1. Why the Internet and digital communications are important

- The Internet is an essential element in 21st century life for education, business and social interaction.

- Internet use is a part of the statutory curriculum and a necessary tool for staff and students.
- Teachers plan Internet use carefully to ensure that it is age-appropriate and supports the learning objectives for specific curriculum areas.
- Staff model safe and responsible behaviour in their own use of technology during lessons.
- Teachers remind students about their responsibilities through an end-user Acceptable Use Policy which every student and parent will sign.
- An Acceptable Use agreement will auto prompt for acceptance at the point of login to PCs and laptops. Students must agree to the conditions before they may proceed.

3.2. Internet use will enhance learning

- The Trust Internet access will be designed expressly for pupil use and will include filtering appropriate to the age of students.
- Students will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.
- Students will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation
- Students will be shown how to publish and present information to a wider audience.

3.3. When accessing the internet, individuals are especially vulnerable to a number of risks which may be physically and emotionally harmful, including:

- Access to illegal, harmful or inappropriate images
- Cyber bullying
- Access to, or loss of, personal information
- Access to unsuitable online videos or games
- Loss of personal images
- Inappropriate communication with others
- Illegal downloading of files
- Exposure to explicit or harmful content, e.g. involving radicalisation
- Plagiarism and copyright infringement
- Sharing the personal information of others without the individual's consent or knowledge

The Trust ensure that e-Safety education is a continuing feature of both staff development and education within schools.

4. Managing Internet Access

4.1. Internet access:

- Internet access will be authorised once parents and students have returned the signed **Acceptable Use Agreement** (Appendix A).
- A record will be kept of all students who have been granted internet access.
- Students' passwords will be changed on a regular basis and their activity is continuously monitored by the **e-Safety Officer**.
- Management systems will be in place to allow teachers and members of staff to control workstations and monitor students' activity.
- Effective filtering systems will be established to eradicate any potential risks to students through access to, or trying to access, certain websites which are harmful or use inappropriate material.
- Filtering systems will be used which are relevant to students' age ranges, their frequency of use of ICT systems, and the proportionality of costs compared to risks.
- The LGC will ensure that use of appropriate filters and monitoring systems does not lead to 'over blocking', such that there are unreasonable restrictions as to what students can be taught with regards to online teaching and safeguarding.
- Any requests by staff for websites to be added or removed from the filtering list must be first authorised by the **Headteacher/Principal**.
- All school systems will be protected by up-to-date virus software.
- An agreed procedure will be in place for the provision of temporary users, e.g. volunteers. These will be applicable to a 24 hour access right, or a set period of time agreed with the **School Business Manager** or **Headteacher/Principal**
- Master users' passwords will be available to the **Headteacher/Principal** for regular monitoring of activity.
- Personal use will only be monitored by the **e-Safety Officer** for access to any inappropriate or explicit sites, where it is justifiable to be necessary and in doing so, would outweigh the need for privacy.

4.2. Information system security

- School ICT systems security will be reviewed regularly.
- Security strategies will be discussed with the Local Authority and Trust.
- Network profiles for each pupil and staff member are created, in which the individual must enter a username and personal password when accessing the ICT systems within the school.

- Passwords have a minimum and maximum length, to prevent 'easy' passwords or mistakes when creating passwords. These will be alpha-numeric and must contain a symbol.
- Passwords will expire after 90 days to ensure maximum security for pupil and staff accounts.
- Passwords should be stored using non-reversible encryption.

4.3. Virus management

- Technical security features, such as virus software, are kept up-to-date and managed by the **e-Safety Officer**.
- The **e-Safety Officer** will ensure that the filtering of websites and downloads is up-to-date and monitored.

4.4. E-safety committee

- The E-safety Policy will be monitored and evaluated by the school's e-Safety committee on a termly basis.
- The committee will include a member of the SLT**, the e-Safety Officer** and the **Designated Safeguarding Lead (DSL)**, as well as members of the LGC.
- Copies of minutes/actions from meetings must be submitted to the Operations Director of HLTY for review.

4.5. Mobile devices and hand-held computers (including tablets and iPads)

- The **Headteacher/Principal** may authorise the use of mobile devices by a pupil where it is seen to be for safety or precautionary use.
- Students are not permitted to access the school's Wi-Fi system at any times using their personal mobile devices and hand-held computers.
- Personal mobile devices are not permitted to be used during school hours by students.
- Students are permitted to use hand-held computers which have been provided or authorised by the school or Trust, though internet access will be monitored for any inappropriate use by the **e-Safety Officer** when using these on the school premises.
- The sending of inappropriate messages or images from mobile devices is prohibited.
- Mobile devices will not be used to take images or videos of students or staff.
- The school will be especially alert to instances of cyber bullying and will treat such instances as a matter of high priority.
- The recording, taking and sharing of images, video and audio on any mobile phone is to be avoided; except where it has been explicitly agreed otherwise by the **Headteacher/Principal**. Such authorised use is to be monitored and recorded.

- The Trust reserves the right to search the content of any mobile or handheld devices on the Trust premises where there is a reasonable suspicion that it may contain undesirable material, including those which promote pornography, violence or bullying. Staff mobiles or hand held devices may be searched at any time as part of routine monitoring.
- Mobile phones and personally-owned mobile devices brought in to the school or Trust are the responsibility of the device owner. The Trust accepts no responsibility for the loss, theft or damage of personally-owned mobile phones or mobile devices.
- The Bluetooth or similar function of a mobile phone should be switched off at all times and not be used to send images or files to other mobile phones.
- No images or videos should be taken on mobile phones or personally-owned mobile devices without the prior written consent of the person or people concerned.
- Mobile Phones and personally-owned devices will be switched off or switched to 'silent' mode during school hours. Bluetooth communication should be 'hidden' or switched off and mobile phones or personally-owned devices will not be used during teaching periods unless permission has been granted by a member of the senior leadership team in emergency circumstances.
- Students' use of personal devices
  - ✓ Hope Learning Trust York strongly advises that student mobile phones should not be brought into school. However, we accept that there may be particular circumstances in which a parent wishes their child to have a mobile phone for their own safety.
  - ✓ If a student breaches Trust policy, then the phone or device will be confiscated and will be held in a secure place in the school office. Mobile phones and devices will be released to parents or carers when agreed by the **Headteacher/Principal**.
  - ✓ If a student needs to contact his or her parents or carers, they will be allowed to use a school phone. Parents are advised not to contact their child via their mobile phone during the school day, but to contact the school office.
  - ✓ Students should protect their phone numbers by only giving them to trusted friends and family members. Students will be instructed in safe and appropriate use of mobile phones and personally-owned devices and will be made aware of boundaries and consequences.

4.6. Email

- Students may only use approved e-mail accounts on the school system.
- The use of personal email accounts to send and receive personal data or information is prohibited.
- No sensitive personal data shall be sent to any other students, staff or third parties via email.
- Students are made aware that all email messages are monitored and that the filtering system will detect inappropriate links, viruses, malware and profanity.

- Any emails sent by students to external organisations will be overseen by their class teacher and must be authorised before sending.
- Chain letters, spam and all other emails from unknown sources must be deleted without opening. The forwarding of chain letters is not permitted.
- Students must immediately tell a teacher if they receive an offensive e-mail.
- In e-mail communication, students must not reveal their personal details or those of others, or arrange to meet anyone without specific permission.
- Incoming e-mail should be treated as suspicious and attachments not opened unless the author is known.
- The Trust:
  - ✓ Does not publish personal e-mail addresses of students or staff on the Trust or individual school websites.
  - ✓ Will contact the Police if one of our staff or students receives an e-mail that we consider is particularly disturbing or breaks the law.
  - ✓ Will ensure that email accounts are maintained and up to date
  - ✓ Reports messages relating to or in support of illegal activities to the relevant Authority and if necessary to the Police.
  - ✓ Knows that spam, phishing and virus attachments can make e mails dangerous.

4.7. Social networking and personal publishing

- Use of social media on behalf of the school will be conducted following the processes outlined in our **Social Media Policy**.
- Access to social networking sites will be filtered as appropriate. Newsgroups will be blocked unless a specific use is approved.
- Should access be needed to social networking sites for any reason, this will be monitored and controlled by staff at all times and must be first authorised by the **Headteacher/Principal**.
- Students are regularly educated on the implications of posting personal data online outside of the school.
- Students will be advised never to give out personal details of any kind which may identify them, their friends or their location.
- Students will be advised to use nicknames and avatars when using social networking sites.
- Teachers are instructed not to run social network spaces for student use on a personal basis or to open up their own spaces to their students, but to use the school's preferred system for such communications.

4.8. Managing filtering

- If students come across unsuitable on-line materials, the site must be reported to the e-Safety Coordinator.
- Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

4.9. Managing videoconferencing & webcam use

- Videoconferencing should use the educational broadband network to ensure quality of service and security.
- Students must ask permission from the supervising teacher before making or answering a videoconference call.
- Videoconferencing and webcam use will be appropriately supervised.

4.10. 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.
- Mobile phones will not be used during school time. The sending of abusive or inappropriate text messages or files by Bluetooth or any other means is forbidden.
- The use by students of cameras in mobile phones will be kept under review.
- Staff will not use personal mobile phones to communicate with children, or use them to capture images of them.

4.11. Protecting personal data

- Personal data will be recorded, processed, transferred and made available as stipulated in the Hope Learning Trust Data Protection Policy. The policy is available on request or can be viewed on line at www.hopelearningtrust.org. This policy complies with GDPR (2018).

5. E-Safety Education

5.1. Educating students

The Trust has a clear, progressive Online safety education programme as part of the Computing curriculum / PSHE curriculum. This covers a range of skills and behaviours appropriate to the age of the children, including:

- ✓ to STOP and THINK before they CLICK
- ✓ to develop a range of strategies to evaluate and verify information before accepting its accuracy;
- ✓ to know how to narrow down or refine a search (KS2);

- ✓ to understand acceptable behaviour when using an online environment / email, i.e. be polite, no bad or abusive language or other inappropriate behaviour; keeping personal information private;
- ✓ to understand why on-line 'friends' may not be who they say they are and to understand why they should be careful in online environments;
- ✓ to understand why they should not post or share detailed accounts of their personal lives, contact information, daily routines, location, photographs and videos and to know how to ensure they have turned-on privacy settings;
- ✓ to have strategies for dealing with receipt of inappropriate materials;
- ✓ to understand why and how some people will 'groom' young people for sexual reasons (KS2);
- ✓ to understand the impact of online bullying, sexting, extremism and trolling and know how to seek help if they are affected by any form of online bullying.
- ✓ to know how to report any abuse including online bullying; and how to seek help if they experience problems when using the Internet and related technologies, i.e. parent or carer, teacher or trusted staff member, or an organisation such as ChildLine or the CLICK CEOP button.

- Teachers plan Internet use carefully to ensure that it is age-appropriate and supports the learning objectives for specific curriculum areas.
- The school will remind students about their responsibilities through a Pupil Acceptable Use Agreement (Appendix A) which every student will sign.
- All staff will model safe and responsible behaviour in their own use of technology during lessons.

5.2. Online risks

- The Trust recognises that students increasingly use a range of technology such as mobile phones, tablets, games consoles and computers. It will support and enable children to use these technologies for entertainment and education but will also teach children (in PSHE) that some adults and young people will use such outlets to harm children.

5.3. Cyber-bullying and abuse

- For the purpose of this policy, cyber bullying is a form of bullying whereby an individual is the victim of harmful or offensive posting of information or images online.
- Complaints of online bullying are dealt with in accordance with our Anti-Bullying Policy. Complaints related to child protection are dealt with in accordance with Trust Child Protection Policy and Procedures.
- Through the PSHE curriculum, children are taught to tell a responsible adult if they receive inappropriate, abusive or harmful e-mails or text messages.
- Posters providing information about how to get help from ChildLine, ThinkUKnow and the NSPCC are displayed in classrooms and along the corridors of the school.

- The school has zero tolerance for cyber bullying, and any incidents will be treated with the upmost seriousness and will be dealt with in accordance with our **Anti-Bullying and Harassment Policy** and **Cyber Bullying Policy**.
- There are clear procedures in place to support anyone in the school community affected by cyberbullying.
- All incidents of cyberbullying reported to the school will be recorded.
- The **Headteacher/Principal** will decide whether it is appropriate to notify the police or anti-social behaviour coordinator in their LA of the action taken against a pupil.

5.4. Sexual exploitation/sexting

- Sexting refers to the sending of sexual messages, including the use of sexually explicit images or videos to another individual via text, apps or other online methods. Sexual exploitation refers to one person using a position or perceived position of power to sexually abuse another, including organised crime, but also covers abuse within relationships.
- Sexting between students will be managed through our anti-bullying and confiscation procedures.
- All staff are made aware of the indicators of sexual exploitation and all concerns are reported immediately to the Designated Safeguarding Lead?
- There are clear procedures in place to support anyone in the Trust community affected by sexting or sexual exploitation.
- All incidents of sexting and sexual exploitation reported to the Trust will be recorded; if necessary the Police will be involved.

5.5. Radicalisation and extremism

- Radicalisation refers to the process by which a person comes to support terrorism and forms of extremism leading to terrorism.
- Extremism is defined by the Crown Prosecution Service as 'The demonstration of unacceptable behaviour by using any means or medium to express views which:
    - Encourage, justify or glorify terrorist violence in furtherance of particular beliefs.
    - Seek to provoke others to terrorist acts.
    - Encourage other serious criminal activity or seek to provoke others to serious criminal acts.
    - Foster hatred which might lead to inter-community violence in the UK.'
- The Trust understands that here is no such thing as a "typical extremist": those who become involved in extremist actions come from a range of backgrounds and experiences, and most individuals, even those who hold radical views, do not become involved in violent extremist activity.

- Trust understands that students may become susceptible to radicalisation through a range of social, personal and environmental factors - it is known that violent extremists exploit vulnerabilities in individuals to drive a wedge between them and their families and communities. It is vital that Trust staff are able to recognise those vulnerabilities.
- Staff will maintain and apply a good understanding of the relevant guidance in order to prevent students from becoming involved in terrorism.
- The Trust will monitor its RE curriculum and assembly policy to ensure that they are used to promote community cohesion and tolerance of different faiths and beliefs.
- Senior leaders will raise awareness within the Trust about the safeguarding processes relating to protecting students from radicalisation and involvement in terrorism.

5.6. Educating parents

- E-safety information will be directly delivered to parents through a variety of formats, including newsletters, the school website and social media.
- Twilight courses and presentations will be run by the school for parents.
- Parents' evenings, meetings and other similar occasions will be utilised to inform parents of any e-Safety related concerns.

6. Communications Policy

6.1. Introducing the e-Safety policy to students

- e-Safety rules and guidance posters will be displayed in corridors and communal spaces and discussed with students regularly. An e-Safety display will be kept up to date in one corridor.
- Students will be informed that network and Internet use will be monitored and appropriately followed up.
- A program of training in e-Safety will be developed by the computing coordinator, PSHE coordinator and safeguarding lead.
- Safety training will be embedded within the computing and PSHE scheme of work in line with National Curriculum expectations.

6.2. Enlisting parents' and carers' support

- Parents' and carers' attention will be drawn to this **e-Safety Policy Acceptable Use Policy**.
- The Trust will maintain a list of e-Safety resources for parents/carers.
- The Trust will ask all new parents to sign the parent /pupil agreement when they register their child with the school.

- The Trust schools will have a page on their websites dedicated to keeping children safe online. It will provide parents with useful links to help them in understanding the internet.

6.3. Advice for parents

- Use internet filtering software such as CyberSentinel, walled gardens and child friendly search engines. Browser controls often offer differing degrees of security for each family member.
- Check out what child protection services your Internet Service Provider (ISP) offers.
- Ensure children are using internet compatible devices in communal areas of the house.
- Tell your children not to give out any personal details. If they want to subscribe to a service (after gaining your permission) make up a family name.
- Make sure your children only use moderated chat rooms, and ask them to introduce you to their online friends.
- Encourage your children to tell you if they feel upset or threatened by what they see online.
- Write a family 'acceptable use policy' for working on the computer.
- Surf together, and be a part of their online life.

7. Published content on the Trust and school websites

7.1. Website security

- The **Headteacher/Principal** will be responsible for the overall content of the website, and will ensure the content is appropriate and accurate.
- Contact details on the school website will include the phone number, email and address of the school – no personal details of staff or students will be published.
- Images and full names of students, or any content that may easily identify a pupil, will be selected carefully, and will not be posted until authorisation from parents has been received.
- Any member of staff that is representing the school online, e.g. through blogging, must express neutral opinions and not disclose any confidential information regarding the school, or any information that may affect its reputability.
- Uploading of information is restricted to the website provider, Trust central team and authorised personnel within each school.
- The Trust and school web site complies with the statutory DfE guidelines for publication on websites.

- Most material is the Trust's own work; where others' work is published or linked to, we credit the sources used and state clearly the author's identity or status.
- The point of contact on the web site is the Trust or school address and telephone number. We use a general email contact address, e.g. hello@hopelearningtrust.org. Home information or individual e-mail identities will not be published.
- Teachers using school approved blogs or wikis will password protect them and run from the school website.

7.2. Publishing pupil's images and work

- Photographs and videos that include students will be selected carefully so that individual students cannot be identified or their image misused.
- Students are not permitted to take or publish photos of others without permission from the individual.
- Students' full names will not be used anywhere on a Trust or school web site or other on-line space, including file names.
- Written consent will be obtained before photographs of students are published on the Trust or school websites.
- Work can only be published with the permission of the pupil and parents/carers.
- Parents should be clearly informed of the Trust policy on image taking and publishing, both on Trust and independent electronic repositories.
- Staff sign the school's Acceptable Use Policy and this includes a clause on the use of mobile phones / personal equipment for taking pictures of students.
- Staff are able to take pictures, though they must do so in accordance with school policies in terms of the sharing and distribution of such. Staff will not take pictures using their personal equipment.
- If specific pupil photos (not group photos) are used on the Trust or school websites, in the prospectus or in other high profile publications the Trust will obtain individual parental or pupil permission for its use.
- The Trust blocks/filter access to social networking sites or newsgroups unless there is a specific approved educational purpose.
- Students are taught about how images can be manipulated in their e-Safety education programme and also taught to consider how to publish for a wide range of audiences which might include governors, parents or younger children as part of their IT scheme of work.
- Students are advised to be very careful about placing any personal photos on any 'social' online network space. They are taught to understand the need to maintain privacy settings so as not to make public, personal information.

- Students are taught that they should not post images or videos of others without their permission. We teach them about the risks associated with providing information with images (including the name of the file), that reveals the identity of others and their location, such as house number, street name or school. We teach them about the need to keep their data secure and what to do if they are subject to bullying or abuse.

8. Reporting misuse

8.1. The Trust will clearly define what is classed as inappropriate behaviour in the Acceptable Use Agreement, ensuring all students are aware of what behaviour is expected of them.

8.2. Inappropriate activities are discussed and the reasoning behind prohibiting activities due to e-Safety are explained to students as part of the curriculum in order to promote responsible internet use.

8.3. Misuse by students:

- Teachers have the power to discipline students who engage in misbehaviour with regards to internet use.
- Any instances of misuse should be immediately reported to a member of staff, who will then report this to the **Headteacher/Principal**, using a **Complaints Form**.
- Any pupil who does not adhere to the rules outlined in our **Acceptable Use Agreement** and is found to be willfully misusing the internet, will have a letter sent to their parents explaining the reason for suspending their internet use.
- Members of staff may decide to issue other forms of disciplinary action to a pupil upon the misuse of the internet. This will be discussed with the **Headteacher/Principal** and will be issued once the pupil is on the school premises.
- Complaints of a child protection nature, such as when a pupil is found to be accessing extremist material, shall be dealt with in accordance with our **Child Protection and Safeguarding Policy**.

8.4. Use of illegal material:

- In the event that illegal material is found on the school's network, or evidence suggest that illegal material has been accessed, the police will be contacted.
- Incidents will be immediately reported to the Internet Watch Foundation and the police will be contacted if the illegal material is, or is suspected to be, a child sexual abuse image hosted anywhere in the world, a non-photographic child sexual abuse image hosted in the UK, or criminally obscene adult content hosted in the UK.
- If a child protection incident is suspected, the school's child protection procedure will be followed – the **Designated Safeguarding Lead** and **Headteacher/Principal** will be informed and the police contacted.

9. Policy Decisions

9.1. Authorising Internet access

- The school will maintain a current record of all students who are granted access to school ICT systems.

9.2. Assessing risks

- The Trust will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a computer connected to the Trust network. The Trust cannot accept liability for any material accessed, or any consequences of Internet access.
- The Trust audit ICT use to establish if the e-Safety policy is adequate and that the implementation of the e-Safety policy is appropriate and effective.

9.3. Handling e-Safety complaints

- Complaints of Internet misuse will be dealt with by a senior member of staff.
- Complaints of a child protection nature must be dealt with in accordance with Trust Child Protection Policy and Procedures. (See Appendix 3)
- Students and parents will be informed of the complaints procedure (see Trust Complaints Policy)
- Students and parents will be informed of consequences for students misusing the Internet.
- Discussions will be held with the Police Youth Crime Reduction Officer to establish procedures for handling potentially illegal issues.

10. Monitoring and review

10.1. The **e-Safety Officer** will evaluate and review this E-Safety Policy on a **termly** basis, taking into account the school's e-Safety calendar, the latest developments in ICT and the feedback from staff/students.

10.2. This policy will also be reviewed on an **annual** basis by the **Hope Learning Trust Resources Committee**; any changes made to this policy will be communicated to all members of staff.

Acceptable Use Agreement: STUDENTS

Class _____

Year _____

Pupil Acceptable Use Agreement

- I will only use ICT in school for School purposes.
- I will only use my own school email address when emailing.
- I will only open email attachments from people I know, or who my teacher has approved.
- I will not tell other people my passwords for the Learning Platform, school network or for other learning websites.
- I will only open/delete my own files.
- I will make sure that all ICT related contact with other children and adults is appropriate and polite.
- I will not deliberately look for, save or send anything that could offend others.
- If I accidentally find anything inappropriate on the internet I will tell my teacher immediately.
- I will not give out my personal details such as my name, phone number, home address or school.
- I will be responsible for my behaviour when using ICT in school or at home because I know that these rules are to keep me safe.
- I know that my use of ICT can be checked and that my parent or carer contacted if a member of staff is concerned about my safety.
- I will not use a mobile phone or other personal ICT device except where it has been specially allowed by the **Headteacher/Principal** or a teacher.

Signature Pupil _____

Signature Parent _____

Date _____

Establishment	E-Safety Officer	Contact Tel. No
Hope Learning Trust	Wendy Munro	01904 560053
Manor Church of England Academy	Louise Scaum	01904 798722
Vale of York Academy	Gavin Kumar	01904 560000
Barlby High School	Vanessa Smallwood/ Phil Cahill	01757 706161
Graham School	Cath Connell	01723 366451
George Pindar School	Blake Murray	01723 582194
Poppleton Ousebank Primary School	Estelle O'Hara	01904 795930
Forest of Galtres Anglican Methodist Primary School	Gemma Sutton	01904 470272
Burton Green Primary School	Ash Atherton/Charlotte Smith-Lynch	01904 552380
Baldersby St James Church of England Primary School	Nigel Stewart	01765 640277
Skelton Primary School	Michaela Carney	01904 555170