HLTY E-SAFETY AND ACCEPTABLE USE POLICY- STAFF & AUTHORISED USERS

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

Document Management:

Date Policy Approved: 02 July 2018
Date Amended: June 2019
Next Review Date: July 2020
Version: 1.4
Approving Body: Resources Committee

Contents:

Statement of intent 2
1. Legal framework 3
2. Roles and responsibilities 3
3. Use of the internet 5
4. Privacy 6
5. Managing Internet Access 6
6. E-Safety 10
7. Published content on the Trust and school websites 12
8. Reporting misuse 14
9. Policy Decisions 14
10. Monitoring and review 15
Appendix A –Acceptable Use Agreement – Staff and Authorised Users 16
Appendix B –Named E-Safety Officers 19
Appendix C – Complaints Form 20

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 teaching and learning, and play an important role in our 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 staff.

The Trust is committed to providing a safe learning and teaching environment for all students, staff and visitors, 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 Hope Learning Trust York community with respect to the use of IT-based technologies.
- safeguard and protect the children and staff 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:

- HLTY Social Media Policy
- HLTY Mobile Phone and Bring Your Own Device (BYOD) Policy
- HLTY Email Policy
- Managing Allegations of Abuse Against Staff Policy
- Technology Acceptable Use Agreement – All Users (**APPENDIX A**)

2. Roles and responsibilities

- This policy applies to members of staff, governors, Trustees, supply teachers, visitors and volunteers (hereafter collectively referred to as "users").
- It is the responsibility of all users 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 **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, staff or visitors.
- The **E-Safety Officer** will ensure that all members of staff are aware of the procedure when reporting e-safety incidents, and will keep a log of all incidents recorded.
- The **E-Safety Officer** will attempt to find alternatives to monitoring staff use of social media, where possible, and will justify all instances of monitoring to ensure that it is necessary and outweighs the need for privacy. The member of staff who is being monitored will be consulted prior to any interception by the school.
- Cyber bullying incidents will be reported in accordance with any associated policy.
- The **E-Safety Officer** will attend **Local Governing Committee (LGC)** meetings termly 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 **E-Safety Officer** and **LGC** will evaluate and review this E-Safety Policy on a **termly** basis, considering 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**, considering new legislation, government guidance and previously reported incidents, to improve procedures.
- Teachers are responsible for ensuring that e-safety issues are embedded in the curriculum and safe internet access is promoted at all times.
- All staff are responsible for ensuring they are up-to-date with current e-safety issues, and this E-Safety Policy.

- All users will ensure they understand and adhere to our **Technology Acceptable Use Agreement – Staff and Visitors.** They must sign and return the form 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.

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.

3.2. 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. Privacy

4.1. The Trust will try to respect your privacy but to protect safety and well-being of students and members of staff, and to protect the Trust from any third-party claims or legal action against it, the Trust may view any data, information or material on the Trust's ICT system (whether contained in an e-mail, on the network, notebooks or laptops). The Trust may, in certain circumstances, disclose that data, information or material to third parties, such as the police or social services. You consent to the Trust viewing, using and disclosing data, information or material in relation to, used, sent or received by you.

4.2. The Trust disclaimer which automatically appears at the end of each of your e-mails notifies the recipient that any e-mail correspondence between is confidential. You must not remove this disclaimer. You should bring to the attention of any person who wishes or intends to send you an e-mail that Trust may monitor the content of their e-mail.

5. Managing Internet Access

5.1. Internet access

- Any requests by users for websites to be added or removed from the filtering list must be first authorised**,** logged and signed off by the **Headteacher/Principal** and available for review.
- All school systems will be protected by up-to-date virus software.
- If necessary, an agreed procedure will be in place for the provision of temporary users, e.g. volunteers. These will be under a 'Guest' procedure.
- Staff can use the internet for personal use outside of their working hours. This must be in line with this E-Safety and Acceptable Use Policy.
- 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.
- Inappropriate internet access by staff may result in disciplinary action.

5.2. Information system security

- School ICT systems security will be reviewed regularly.
- Virus protection will be updated regularly.
- Security strategies will be discussed with the Trust Board.
- Network profiles for each 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.

- Passwords will expire after 90 days to ensure maximum security for student and staff accounts.
- Passwords for guest accounts will be applicable for 24 hours, unless otherwise agreed and authorised by the **Headteacher/Principal**.
- Passwords should be stored using non-reversible encryption.

5.3. 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.

5.4. Mobile phones, hand-held computers and mobile devices

- Use of mobile devices on behalf of the school will be conducted following the processes outlined in the **HLTY Mobile Phone and BYOD Policy**.
- Staff are permitted to use mobile devices, laptops or PCs which have been provided by the school, though internet access will be monitored for any inappropriate use by the **E-Safety Officer** when using these on the school premises.
- The use of non-school or Trust provided devices (including personal smartphones) to access school or Trust email accounts is strictly prohibited unless registered with the academy/school in accordance with the **HLTY Mobile Phone and BYOD Policy**. This includes adding a school or Trust email account to an existing app on a smartphone or personal tablet, and to logging in to work email accounts from a personal device such as laptop or PC.
- The sending of inappropriate messages or images from mobile devices is prohibited.
- Personal mobile devices will not be used to take images or videos of students or staff in accordance with the **HLTY Mobile Phone and BYOD Policy**.
- The school will be especially alert to instances of cyber bullying and will treat such instances as a matter of high priority.
- If a mobile phone is necessary for instance in case of emergency during off-site activities, or for contacting students or parents, then a school or Trust mobile phone will be provided and used. In an emergency where a staff member doesn't have access to a Trust owned device, they should use their own device and hide (by inputting 141) their own mobile number for confidentiality purposes.
- Staff may use their personal mobile devices during break times and out of school hours. If a classroom-based staff member is expecting an urgent personal call they may leave their phone with the office to answer on their behalf, or seek specific permissions to use their phone at a time other than their break times.

5.5. E-mail

- Staff will be given approved email accounts where appropriate and are only able to use these accounts, in accordance with **HLTY Emails Policy and Procedure**.
- The use of personal email accounts to send and receive personal data or information is prohibited on school equipment.
- Staff must ensure that confidential emails are suitably protected at all times. If working at home or remotely, you should be aware of the potential for an unauthorised third party to be privy to the content of the email. Confidential emails should be deleted when no longer required.
- Staff members are aware that their email messages can be monitored.
- Chain letters, spam and all other emails from unknown sources must be deleted without opening. The forwarding of chain letters is not permitted.
- Incoming e-mail should be treated as suspicious and attachments not opened unless the author is known.
- E-mails remain a written record and can be forwarded to others or printed for formal use, for example in Subject Access Requests.
- As a rule, staff should be well advised to only write what they would say face to face and should avoid the temptation to respond to an incident or message by e-mail in an uncharacteristic and potentially aggressive fashion. Remember "Tone" can be misinterpreted on the printed page and once it is sent it could end up in the public domain forever. Email lacks the other cues and clues that convey the sense in which what you say is to be taken, and you can easily convey the wrong impression.
- Email sent from a **Trust** account is similar to sending a letter on **Trust** letterhead. Staff must not say anything that might bring discredit or embarrassment to themselves or the Trust.
- The Trust:
  - ✓ Provides staff with an email account for their professional use (Microsoft Office) and makes clear that personal email should be through a separate account.
  - ✓ Does not publish personal e-mail addresses of students or staff on the Trust/ academy/school websites.
  - ✓ Will contact the Police if one of our staff or students receives an electronic communication that we consider is potentially illegal.
  - ✓ 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.

5.6. Social networking and personal publishing

- Use of social media on behalf of the school will be conducted following the processes outlined in the **HLTY Social Media Policy**.
- Access to social networking sites will be filtered as appropriate.
- 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**.
- Staff are regularly educated on posting inappropriate photos or information online, which may potentially affect their position and the school as a whole.
- Staff are not permitted to communicate with students over social networking sites and are reminded to alter their privacy settings.
- Staff are not permitted to publish comments about the school which may adversely affect its reputation.
- Staff are not permitted to access social media sites during teaching hours unless it is justified to be beneficial to the material being taught. This will be discussed with the **Headteacher/Principal** prior to accessing the social media site.
- Newsgroups will be blocked unless a specific use is approved.
- Staff advised not to accept/add parents or students as 'friends' on social networking sites unless a signed declaration has been submitted and approved by the **Headteacher/Principal**.
- Staff will be shown how to 'block' their profile picture from being downloaded and protect their profile information.
- Staff will be encouraged to 'un-tag' themselves from any inappropriate pictures that may appear on 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 should use the school's preferred system for such communications.
- Trust staff will ensure that in private use:
  - ✓ No reference should be made in social media to students, parents / carers or staff
  - ✓ They do not engage in online discussion on personal matters relating to members of the Trust or school community
  - ✓ Personal opinions should not be attributed to the Trust, school or local authority
  - ✓ Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

6. E-Safety

6.1. 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** where appropriate.

6.2. Managing filtering

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

6.3. 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.
- The Senior Leadership Team should note that technologies such as mobile phones with wireless Internet access can bypass Trust filtering systems and present a new route to undesirable material and communications.

6.4. 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 online at **http://hopelearningtrust.org/key-information-and-policies/** This policy complies with GDPR (2018).

6.5. Education

- 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 Student Acceptable Use Agreement which every student will sign. The **HLTY E-Safety and Acceptable Use Policy for Students** and **Acceptable Use Agreement -Students** are available to view or download at: **http://hopelearningtrust.org/key-information-and-policies/**
- All staff will model safe and responsible behaviour in their own use of technology during lessons.

6.6. 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.

  The school will regularly educate staff, students and parents on the importance of staying safe online, as well as being considerate to what they post online.

- The school will commit to creating a learning and teaching environment which is free from harassment and bullying, ensuring the happiness of all members of staff and students.
- 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 all relevant policies
- Complaints related to child protection are dealt with in accordance with Trust / LA child protection procedures.
- There are clear procedures in place to support anyone in the Trust community affected by cyberbullying.
- All incidents of cyberbullying reported to the Trust will be recorded.

6.7. Sexual exploitation/sexting

- All staff are made aware of the indicators of sexual exploitation and all concerns are reported immediately to the DSL.
- There are clear procedures in place to support anyone in the Trust community affected by sexting.
- All incidents of sexting reported to the Trust will be recorded.

6.8. 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.

- The 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.

6.9. Educating staff

- A planned calendar programme of e-safety training opportunities is available to all staff members, including whole school activities and CPD training courses.
- All staff will undergo e-safety training on a **termly** basis to ensure they are aware of current e-safety issues and any changes to the provision of e-safety, as well as current developments in social media and the internet as a whole.
- All staff will undergo regular audits by the **E-Safety Officer** in order to identify areas of training need.
- All staff will employ methods of good practice and act as role models for students when using the internet and other digital devices.
- All staff will be educated on which sites are deemed appropriate and inappropriate.
- All staff are reminded of the importance of acknowledging information they access online, in order to avoid copyright infringement and/or plagiarism.
- Any new staff are required to undergo e-safety training as part of their induction programme, ensuring they fully understand this E-Safety Policy.
- The **E-Safety Officer** will act as the first point of contact for staff requiring e-safety advice.

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, and name and email address of key members of personnel to contact as required by DfE – no personal contact details of staff or students will be published.

- 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 adversely affect its reputation.
- 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 will not be published. Individual e-mail identities linking to Trust/academy will only be used when required by law or strongly advised by ICO, DfE or Ofsted.
- Teachers using school approved blogs or wikis will password protect them and run from the school website.

7.2. Publishing students' images and work

- Photographs and videos that include students will only be published with consent according to **HLTY Photographs and Videos in Schools Policy.** Full details can be accessed at http://hopelearningtrust.org/key-information-and-policies/
- 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 **Technology Acceptable Use Agreement (Appendix A)** 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 student 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 student permission for its use.
- The Trust blocks/filter access to social networking sites or newsgroups unless there is a specific approved educational purpose.

8. Reporting misuse

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

8.2. Misuse by staff:

- Any misuse of the internet by a member of staff should be immediately reported to the **Headteacher/Principal**, using a **Complaints Form (Appendix C)**.
- The **Headteacher/Principal** will deal with such incidents in accordance with the **Managing Allegations of Abuse Against Staff Policy**, and may decide to take disciplinary action against the member of staff.
- 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 member of staff.

8.3. 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

- All staff and authorised users must read and sign the '**Technology Acceptable Use Agreement'** (Appendix A) before using any school or Trust ICT resource.
- The Trust will maintain a current record of all staff who are granted access to Trust 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.
- Any complaint about staff misuse must be referred to the **Headteacher/Principal**.
- Complaints of a child protection nature must be dealt with in accordance with Trust child protection procedures.

10. Monitoring and review

- The **E-Safety Committee** 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.
- This policy will also be reviewed on an **annual** basis by the **Trust Board Resources Committee**; any changes made to this policy will be communicated to all members of staff.
- Members of staff are required to familiarise themselves with this policy as part of their induction programmes.

Acceptable use agreement – Staff and Authorised Users

Name of school: **Date:**

Whilst our school promotes the use of technology, and understands the positive effects it can have on enhancing students' learning and community engagement, we must also ensure that staff use technology appropriately. Any misuse of technology will not be taken lightly, and will be reported to the **Headteacher/Principal** in order for any necessary further action to be taken.

This acceptable use agreement is designed to outline staff responsibilities when using technology, whether this is via personal devices or school devices, or on/off the school premises, and applies to all staff, volunteers, contractors and visitors.

Please read this document carefully, and sign below to show you agree to the terms outlined.

1. **Using technology in school**

- I will only use ICT systems, such as computers (including laptops) and tablets, which have been permitted for my use by the **Headteacher/Principal**.
- I will only use the approved email accounts that have been provided to me.
- I will not use personal emails to send and receive personal data or information.
- I will not share sensitive personal data with students, staff or third parties.
- I will ensure that any personal data is stored in line GDPR 2018.
- I will delete any chain letters, spam and other emails from unknown sources without opening them.
- I will ensure that I obtain permission prior to accessing learning materials from unapproved sources.
- I will only use the internet for personal use during out-of-working hours, including break and lunch times.
- I will not search for, view, download, upload or transmit any explicit or inappropriate material when using the internet.
- I will not share school-related passwords with students, staff or third parties unless permission has been given for me to do so.
- I will not install any software onto school ICT systems unless instructed to do so by the **E-Safety Officer** or **Headteacher/Principal**.
- I will only use recommended and encrypted removable media, and will keep this securely stored.
- I will provide removable media to the **E-Safety Officer** for safe disposal once I am finished with it.

2. Mobile devices

- I will only use school/academy/Trust-owned mobile devices for educational purposes.
- I will not use personal mobile or other devices for school/academy/Trust purposes.
- I will only use personal mobile devices during out-of-working hours, including break and lunch times.
- I will not access school/academy/Trust email content on a personal mobile device, including personal PC/Laptop unless I have registered the device with the school/academy in accordance with the Bring Your Own Device (BYOD) Policy.
- I will not access school/academy/Trust email content on a PC or laptop that is not owned by the school/academy/Trust unless I have registered the device with the school/academy in accordance with the Bring Your Own Device (BYOD) Policy.
- I will ensure that mobile devices are either switched off or set to silent mode during school hours, and will only make or receive calls in specific areas permitted by the **Headteacher/Principal**, e.g. the staffroom.
- I will ensure mobile devices are kept on 'silent' and stored in a secure location during lesson times.
- I will not use personal mobile devices to take images or videos of students or staff – I will seek permission from the **Headteacher/Principal** before any school-owned mobile device is used to take images or recordings.
- I will not use mobile devices to send inappropriate messages, images or recordings.
- I will ensure that personal and school-owned mobile devices do not contain any inappropriate or illegal content.
- I will not access the Wi-Fi system using personal mobile devices, unless permission has been given by the **Headteacher/Principal** or **E-Safety Officer**.
- I will not use personal and school-owned mobile devices to communicate with students or parents **except**:
- In case of emergency **only**, (in circumstances whereby no alternative form of communication is available) I understand that a mobile can be used; Caller ID **must** be withheld by adjusting the settings or place 141 in front of the number. The data i.e. telephone number must be deleted from the mobile phone call history. A written notification to the Headteacher/Principal **must** be given as soon as possible after the event explaining the circumstances and confirming that all personal data has been deleted from the device.
- I will ensure that any school data stored on personal mobile devices is password protected, and give permission for the **E-Safety Officer** to erase and wipe data off my device if it is lost or as part of exit procedures.

3. Social media and online professionalism

- If I am representing the school online, e.g. through blogging, I will express neutral opinions and will not disclose any confidential information regarding the school, or any information that may affect its reputability.
- I will not use any school or Trust-owned mobile devices to access social networking sites, unless it is beneficial to the material being taught; or is part of my role in the school or Trust.
- I will not communicate with students or parents over personal social networking sites.
- I will not accept 'friend requests' from any students or parents over social networking sites.

- I will ensure that I apply the necessary privacy settings to my social networking sites.
- I will not publish any comments or posts about the school on my social networking sites which may affect the school's reputability.
- I will not post or upload any defamatory, objectionable, copyright infringing or private material, including images and videos of students, staff or parents, on any online website.
- I will not give my home address, phone number, mobile number, social networking details or email addresses to students or parents – any contact with parents will be done through authorised school contact channels.

4. Training

- I will ensure I participate in any e-safety or online training offered to me, and will remain up-to-date with current developments in social media and the internet as a whole.
- I will ensure that I allow the **E-Safety Officer** to undertake regular audits to identify any areas of need I may have in relation to training.
- I will ensure I employ methods of good practice and act as a role model for students when using the internet and other digital devices.
- I will ensure that I deliver any training to students as required.

5. Reporting misuse

- I will ensure that I adhere to any responsibility I have for monitoring, as outlined in the **Acceptable Use and E-Safety Policy**, e.g. to monitor students' internet usage.
- I will ensure that I report any misuse by students, or by staff members breaching the procedures outlined in this agreement, to the **Headteacher/Principal**.
- I understand that my use of the internet will be monitored by the **E-Safety Officer** and recognise the consequences if I breach the terms of this agreement.
- I understand that the **Headteacher/Principal** may decide to take disciplinary action against me in accordance with the **Allegations of Abuse Against Staff Policy** if I breach this agreement.

I certify that I have read and understood this agreement, and ensure that I will abide by each principle.

Signed: Date:
(Staff Member)

Print name:

Signed: Date:
(Line Manager)

Print name

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

COMPLAINTS FORM

Please complete and return to the Headteacher/Principal, who will acknowledge receipt and explain what action will be taken.

Your Name:
Address:
Postcode:
Day time telephone number:
Evening telephone number:
Please give details of your complaint, and the name of any person(s) the complaint concerns. **(Continue on to additional sheet if necessary)**
What action, if any, have you already taken to try and resolve your complaint. **(Who did you speak to and what was the response)?**

What actions do you feel might resolve the problem at this stage?
Are you attaching any paperwork/evidence? If so, please give details.
Signature of complainant:_____ Date_____
Official use **Acknowledgement sent by (Name):_____ Date_____** **Complaint referred to (Name):_____ Date_____** **Resolution (details):**
Signature:_____ Date:_____