Hope School and College

# IT - Acceptable Use Policy

Ratified On :

Review Date: September 2026

**Pupils Acceptable Use Policy: Sample Statements**

Although the statements for children are collected within key stages it is recommended that schools and settings amend and adapt them according to their own cohorts as appropriate. Schools and settings will also need to adapt these templates in line with their own technology use e.g. the expectations or requirements may vary if schools use laptops or tablets.

Some useful links to assist with e-safety online can be found at http://www.kelsi.org.uk/child-protection-and-safeguarding/e-safety/e-safety-classroom-materials .

**EYFS (3 – 5)**

- I only go online with a grown up
- I am kind online
- I keep information about me safe online
- I tell a grown up if something online makes me unhappy or worried

**KS1 (5-7)**

- I only use the internet when an adult is with me
- I only click on links and buttons when I know what they do
- I keep my personal information and passwords safe online
- I only send messages online which are polite and friendly
- I know the school can see what I am doing online
- I know that I cannot use my own device in school
- I know that if I do not follow the rules then:
    - My use of computing facilities maybe subject to closer scrutiny and monitoring and/or I could be restricted in use or banned from using facilities for a period of time
    - My parents/carers may be contacted if there are concerns about my conduct
    - Serious incidents may mean other agencies are contacted (e.g. Police, Social Services)

- I have read and talked about these rules with my parents/carers
- I always tell an adult/teacher if something online makes me feel unhappy or worried
- I can visit www.thinkuknow.co.uk to learn more about keeping safe online

**Early Years and KS1 Acceptable Use Poster**

**KS2 Pupils (7-11)**

- I always ask permission from an adult before using the internet
- I only use websites and search engines that my teacher has chosen
- I use my school computers for school work unless I have permission otherwise
- I understand that my own personal devices/mobile phone are not to be used in school
- I know that not everything or everyone online is honest or truthful and will check content on other sources like other websites, books or with a trusted adult
- I always credit the person or source that created any work, image or text I use
- I only talk with and open messages from people I know and I only click on links if I know they are safe
- I always talk to an adult if I'm not sure about something or if something happens online that makes me feel worried or frightened
- I only send messages which are polite and friendly
- I keep my personal information safe and private online
- I will keep my passwords safe and not share them with anyone
- I will not access or change other peoples' files or information
- I will only post pictures or videos on the Internet if they are appropriate and if I have permission
- I will only change the settings on the computer if a teacher/technician has allowed me to
- I understand that the school's internet filter is there to protect me, and I will not try to bypass it.
- I know that people I meet online may not always be who they say they are. If someone online suggests meeting up, I will immediately talk to an adult
- I know that my use of school devices/computers and Internet access will be monitored
- I know that I should report any damage to school devices/computers to my teacher
- I know I should only use and access my own shared file storage areas
- I know I should only use my own cloud computing area (e.g. Google Education/Apple Teach)
- I know that if I do not follow the rules then:
    - My use of computing facilities maybe subject to closer scrutiny and monitoring and/or I could be restricted in use or banned from using facilities for a period of time
    - My parents/carers may be contacted if there are concerns about my conduct
    - Serious incidents may mean other agencies are contacted (e.g. Police, Social Services)
- If I see anything online that I shouldn't or that makes me feel worried or upset then I will minimise the page and tell an adult straight away.
- I have read and talked about these rules with my parents/carers
- If I am aware of anyone being unsafe with technology then I will report it to a teacher
- I can visit www.thinkuknow.co.uk and www.childline.org.uk to learn more about keeping safe online

**KS2 Shortened version (for use on posters etc)**

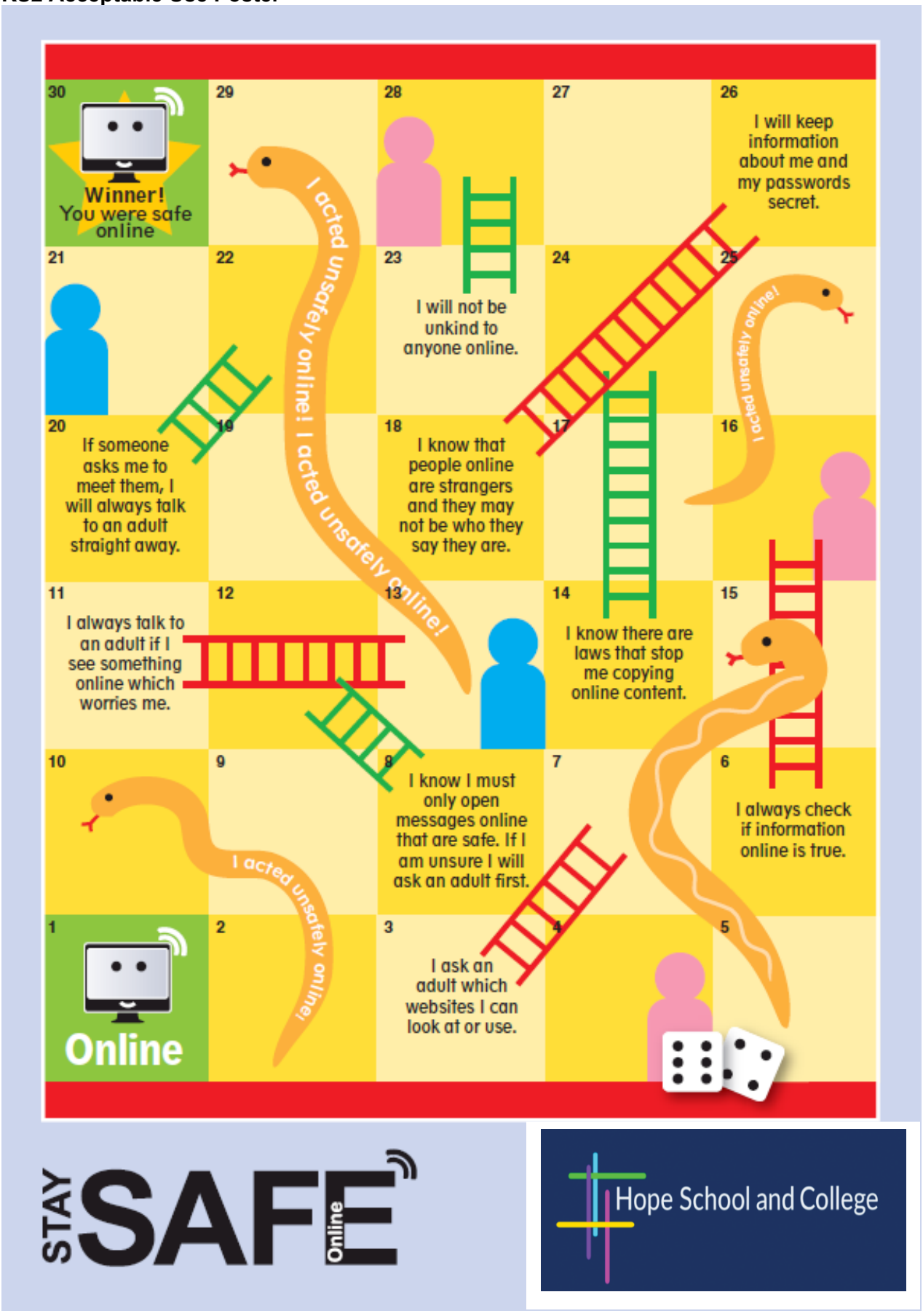
- I ask adult which websites I can use
- I will not assume information online is true
- I know there are laws that stop me copying online content
- I know I must only open online messages that are safe and if I'm unsure then I won't open it without speaking to an adult first
- I know that people online are strangers and they may not always be who they say they are
- If someone online suggests meeting up then I will always talk to an adult straight away

- I will not use technology to be unkind to people
- I will keep information about me and my passwords private
- I always talk to an adult if I see something which makes me feel worried

**Alternative KS2 Statements**

- I know that I will be able to use the internet in school, for a variety of reasons, if I use it responsibly. However, I understand that if I do not, I may not be allowed to use the internet at school.
- I know that being responsible means that I should not look for bad language, inappropriate images or violent or unsuitable games, and that if I accidently come across any of these, I should report it to a teacher or adult in school or a parent or carer at home.
- I will treat my password like my toothbrush! This means I will not share it with anyone (even my best friend), and I will log off when I have finished using the computer or device.
- I will protect myself by never telling anyone I meet online my address, my telephone number, my school's name or by sending a picture of myself without permission from a teacher or other adult.
- I will never arrange to meet anyone I have met online alone in person without talking to a trusted adult.
- If I get unpleasant, rude or bullying emails or messages I will report them to a teacher or other adult. I will not delete them straight away, but instead, keep them so I can show them to the person I am reporting it to.
- I will always be myself and not pretend to be anyone or anything I am not. I know that posting anonymous messages or pretending to be someone else is not allowed.
- I will always check before I download software or data from the internet. I know that information on the internet may not be reliable and it sometimes needs checking.
- I will be polite and sensible when I message people online and I know that sending a message is the same as having a conversation with someone. I will not be rude or hurt someone's feelings online.
- I know that I am not allowed on personal e-mail, social networking sites or instant messaging in school.
- If, for any reason, I need to bring my mobile phone into school I know that it is to be handed in to the office and then collected at the end of the school day.
- I will tell a teacher or other adult if someone online makes me feel uncomfortable or worried when I am online using games or other websites or apps.

**KS2 Acceptable Use Poster**




STAY SAFE Online

Hope School and College

**Possible Statements for Children with Special Educational Needs and Disabilities** (These statements are based on ability levels rather than age)

**Children and Young People functioning at Levels P4 –P7**

- I ask a grown up if I want to use the computer
- I make good choices on the computer
- I use kind words on the internet
- If I see something, I don't like online I tell a grown up
- I know that if I do not follow the school rules then:
    - My use of computing facilities maybe subject to closer scrutiny and monitoring and/or I could be restricted in use or banned from using facilities for a period of time
    - My parents/Carers may be contacted if there are concerns about my conduct
    - Serious incidents may mean other agencies are contacted (e.g. Police, Social Services)

**Children functioning at Levels P7-L1** (Based on Childnet's SMART Rules: www.childnet.com )

**Safe**

- I ask a grown up if I want to use the computer
- On the internet I don't tell strangers my name
- I know that if I do not follow the school rules then

**Meeting**

- I tell a grown up if I want to talk on the internet

**Accepting**

- I don't open emails from strangers

**Reliable**

- I make good choices on the computer

**Tell**

- I use kind words on the internet
- If I see something, I don't like then I tell a grown up

**Children and Young People functioning at Levels L2-4** (Based on SMART Rules: www.childnet.com)

**Safe**

- I ask an adult if I want to use the internet
- I keep my information private on the internet
- I am careful if I share photos online
- I know that if I do not follow the school rules then the behaviour policy will apply

**Meeting**

- I tell an adult if I want to talk to people on the internet
- If I meet someone online, I talk to an adult

**Accepting**

- I don't open messages from strangers
- I check web links to make sure they are safe

**Reliable**

- I make good choices on the internet
- I check the information I see online

**Tell**

- I use kind words on the internet
- If someone is mean online then I don't reply, I save the message and show an adult
- If I see something online, I don't like then I tell an adult

**Parent/Carers Acceptable Use Policy Statements**

- I have read and discussed the Acceptable Use Policy (attached) with my child
- I know that my child will receive online safety (e-Safety) education to help them understand the importance of safe use of technology and the internet, both in and out of school.
- I am aware that any internet and computer use using school equipment may be monitored for safety and security reasons and to safeguard both my child and the schools' systems. This monitoring will take place in accordance with data protection and human rights legislation.
- I understand that the school will take all reasonable precautions to ensure that pupils cannot access inappropriate materials but I appreciate that this is a difficult task.
- I understand that if the school has any concerns about my child's safety online, either at school or at home, then I will be contacted
- I understand that if my child does not abide by the school Acceptable Use Policy then sanctions will be applied in line with the schools behaviour and anti-bullying policy. If the school believes that my child has committed a criminal offence then the Police will be contacted
- I, together with my child, will support the school's approach to online safety (e-Safety) and will not deliberately upload or add any images, video, sounds or text that could upset, threaten the safety of or offend any member of the school community
- I know that I can speak to the school Online Safety (e-Safety) Coordinator (Insert Name), my child's teacher or the Head Teacher if I have any concerns about online safety (e-Safety)
- I will visit the school website (https://www.hope.wigan.sch.uk/about/policies/) for more information about the school's approach to online safety as well as to access useful links to support both myself and my child in keeping safe online at home
- I will visit www.thinkuknow.co.uk/parents, www.nspcc.org.uk/onlinesafety, www.internetmatters.org www.saferinternet.org.uk and www.childnet.com for more information about keeping my child(ren) safe online
- I will support the school and my child by role modelling safe and positive online behaviour (such as sharing images, text and video responsibly) and by discussing online safety with them when they access technology at home

**I have read the Parent Acceptable Use Policy**.

Child's Name…….. Class……

Parents Name…….....Parents Signature…….

Date…….

**Use of Cloud Systems Permission Form**

The school uses Google Apps for Education and other 'Cloud' based computing platforms (Apple Classroom, Class Dojo, Padlet etc.) for pupils and staff. This consent form describes the tools and pupil responsibilities for using these services.

The following services are available to each pupils and hosted by Google as part of the school's online presence in Google Apps for Education

- **Mail** - an individual email account for school use managed by the school
- **Calendar** - an individual calendar providing the ability to organize schedules, daily activities, and assignments
- **Docs** - a word processing, spreadsheet, drawing, and presentation toolset that is very similar to Microsoft Office
- **Sites** - an individual and collaborative website creation tool

Using these tools and others on other platforms, pupils collaboratively create, edit and share files and websites for school related projects and communicate via email with other pupils and members of staff. These services are entirely online and available 24/7 from any Internet-connected computer. Examples of student use include showcasing class projects, building an electronic portfolio of school learning experiences, and working in small groups on presentations to share with others.

(The school has policies and procedures to safeguard your child when online, we have robust data protection, children are taught about staying safe online and acceptable use of systems, children are supervised when using school systems. These policies and procedures will be added to and reconsidered if and when needed)

The school believes that use of the tools significantly adds to your child's educational experience.

As part of the Google terms and conditions we are required to seek your permission for your child to have a Google Apps for Education account:

**Use of Cloud Storage Systems – Parental Consent**

Child's Name……. Class……

Parents Name……..

Parents Signature…….

Date…….

*The Department for Education has published advice and information regarding Cloud (educational apps) software services and the Data Protection Act here:*
*https://www.gov.uk/government/publications/cloud-software-services-and-the-data-protection-act*

Dear Parent/Carer

All pupils use computer facilities including Internet access as an essential part of learning, as required by the National Curriculum. Your child will have the opportunity to access a wide range of information and communication technology (ICT) resources. This includes access to:

- Computers, laptops and other digital devices
- Internet which may include search engines and educational websites
- School learning platform/intranet
- Email
- Games consoles and other games-based technologies
- Digital cameras, web cams and video cameras
- Recorders and Dictaphones
- Mobile Phones and Smartphone's

Hope School and College recognise the essential and important contribution that technology plays in promoting children's learning and development and offers a fantastic range of positive activities and experiences. However, we also recognise there are potential risks involved when using online technology and therefore have developed online safety (e-Safety) policies and procedures alongside the schools safeguarding measures.

The school takes responsibility for your child's online safety very seriously and, as such, we ensure that pupils are educated about safe use of technology and will take every reasonable precaution to ensure that pupils cannot access inappropriate materials whilst using school equipment. However, no system can be guaranteed to be 100% safe and the school cannot be held responsible for the content of materials accessed through the internet and the school is not liable for any damages arising from use of the schools' internet and ICT facilities.

Full details of the school's Acceptable Use Policy and online safety (e-Safety) policy are available on the school website (https://www.hope.wigan.sch.uk/about/policies/) or on request.

We request that all parents/carers support the school's approach to online safety (e-Safety) by role modelling safe and positive online behaviour for their child and by discussing online safety with them whenever they access technology at home. Parents/carers can visit the school website's (https://www.hope.wigan.sch.uk/about/policies/) for more information about the school's approach to online safety as well as to access useful links to support both you and your child in keeping safe online at home. Parents/carers may also like to visit www.thinkuknow.co.uk, www.childnet.com, www.nspcc.org.uk/onlinesafety, www.saferinternet.org.uk and www.internetmatters.org for more information about keeping children safe online

Whilst the school monitors and manages technology use in school we believe that children themselves have an important role in developing responsible online behaviours. In order to support the school in developing your child's knowledge and understanding about online safety, we request that you read the attached Acceptable Use Policy with your child and that you and your child discuss the content and return the attached slip. Hopefully, you will also find this Acceptable Use Policy provides you with an opportunity for conversations between you and your child about safe and appropriate use of the technology, both at school and at home.

Should you wish to discuss the matter further, please do not hesitate to contact the school online safety Coordinator (Insert Name) or myself.

**Early Years/KS1/SEN**
We understand that your child is too young to give informed consent on his/ her own; however, we feel it is good practice to involve them as much as possible in the decision-making process, and believe a shared commitment is the most successful way to achieve this.

Yours sincerely,

Insert Name
Headteacher

**Parent/Carer Acceptable Use Policy Acknowledgement Form**

**Pupil Acceptable Use Policy – Hope School and College Parental Acknowledgment**

I, with my child, have read and discussed Hope School and College Pupil Acceptable Use Policy.

I, with my child understand there may be a need to set my child up to be able to login to email and educational systems. I, with my child, understand that the login will consist of our family name and their initial

I am aware that any internet and computer use using school equipment may be monitored for safety and security reason to safeguard both my child and the schools' systems. This monitoring will be proportionate and will take place in accordance with data protection, privacy and human rights legislation.

I with my child, am aware of the importance of safe online behaviour and will not deliberately upload or add any images, video, sounds or text that could upset, threaten the safety of or offend any member of the school community.

I understand that the school will take all reasonable precautions to ensure that pupils cannot access inappropriate materials but I appreciate that this is a difficult task. I understand that the school will take all reasonable precautions to reduce and remove risks but cannot ultimately be held responsible for the content of materials accessed through the Internet.

I understand that the school will contact me if they have concerns about any possible breaches of the Acceptable Use Policy or have any concerns about my child's safety.

I will inform the school or other relevant organisations if I have concerns over my child's or other members of the school communities' safety online.

I know that my child will receive online safety education to help them understand the importance of safe use of technology and the internet – both in and out of school.

I will support the schools e-Safety approaches and will encourage my child to adopt safe use of the internet and digital technologies at home.

Child's Name…… Signed (if appropriate) ……..

Class…… Date……..

**Letter for Staff**

Dear Colleague

Social media can blur the definitions of personal and working lives, so it is important that all members of staff take precautions in order to protect themselves both professionally and personally online.

Be very conscious of both your professional reputation and that of the school when you are online. All members of staff are strongly advised, in their own interests, to take steps to ensure that their personal information and content is not accessible to anybody who does not or should not have permission to access it. All staff must also be mindful that any content shared online cannot be guaranteed to be "private" and could potentially be seen by unintended audiences which may have consequences including civil, legal and disciplinary action being taken. Ensure that your privacy settings are set appropriately (many sites have a variety of options to choose from which change regularly and may be different on different devices) as it could lead to your content accidentally being shared with others.

Be very careful when publishing any information, personal contact details, video or images etc online; ask yourself if you would feel comfortable about a current or prospective employer, colleague, child in your care or parent/carer, viewing or sharing your content. If the answer is no, then consider if it should be posted online at all. It is very important to be aware that sometimes content shared online, even in jest, can be misread, misinterpreted or taken out of context, which can lead to complaints or allegations being made. Don't be afraid to be yourself online but do so respectfully. All staff must be aware that as professionals, we must be cautious to ensure that the content we post online does not bring the school or our professional role into disrepute.

If you have a social networking account, it is advised that you do not to accept pupils (past or present) or their parents/carers as "friends" on a personal account. You may be giving them access to your personal information and allowing them to contact you inappropriately through unregulated channels. They may also be giving you access to their personal information and activities which could cause safeguarding concerns. Please use your work provided email address or phone number to contact children and/or parents – this is essential in order to protect yourself as well as the wider community. If you have a pre-existing relationship with a child or parent/carer that may compromise this or have any queries or concerns about this then please speak to the Online safety (e-Safety) Coordinator (insert name) or Designated Safeguarding Lead /Manager (Insert Name).

Documents called "Cyberbullying: Supporting School Staff", "Cyberbullying: advice for headteachers and school staff" and "Safer professional practise with technology" are available in the staffroom and are stored on the staff drive in the E Safety folder. Please photocopy them if you want or download the documents directly from www.childnet.com, www.e-safety.org.uk and www.gov.uk/government/publications/preventing-and-tackling-bullying. Staff can also visit or contact the Professional Online safety Helpline www.saferinternet.org.uk/about/helpline for more advice and information on online professional safety.

I would like to remind all staff of our Acceptable Use Policy and the importance of maintaining professional boundaries online. Failure to follow this guidance and the school policy could lead to disciplinary action, so it is crucial that all staff understand how to protect themselves online. Please speak to your line manager, the Designated Safeguarding Leads (Insert DDSL, [Insert DSL]) or myself if you have any queries or concerns regarding this.

Yours sincerely,

[Insert Head teachers Name]

Headteacher

**Additional content for staff regarding online participation on behalf the School**

The principles and guidelines below set out the standards of behaviour expected of you as an employee of the school. If you are participating in online activity as part of your capacity as an employee of the school then we request that you:

- Be professional and remember that you are an ambassador for the school. Disclose your position but always make it clear that you do not necessarily speak on behalf of the school.
- Be responsible and honest at all times and consider how the information you are publishing could be perceived
- Be credible, accurate, fair and thorough.
- Always act within the legal frameworks you would adhere to within school, including libel, defamation, confidentiality, copyright, data protection as well as equalities laws.
- Be accountable and do not disclose information, make commitments or engage in activities on behalf of the school unless you are authorised to do so.
- Always inform your line manager, the designated safeguarding lead and/or the head teacher of any concerns such as criticism or inappropriate content posted online.

**Hope School and College Staff Acceptable Use Policy 2019**

As a professional organisation with responsibility for children's safeguarding it is important that all staff take all possible and necessary measures to protect data and information systems from infection, unauthorised access, damage, loss, abuse and theft. All members of staff have a responsibility to use the school's computer system in a professional, lawful, and ethical manner. To ensure that members of staff are fully aware of their professional responsibilities when using Information Communication Technology and the school systems, they are asked to read and sign this Acceptable Use Policy.

This is not an exhaustive list and all members of staff are reminded that ICT use should be consistent with the school ethos, other appropriate school policies, relevant national and local guidance and expectations, and the Law.

1. I understand that Information Systems and ICT include networks, data and data storage, online and offline communication technologies and access devices. Examples include laptops, mobile phones, tablets, digital cameras, email and social media sites**.**

2. School owned information systems must be used appropriately. I understand that the Computer Misuse Act 1990 makes the following criminal offences: to gain unauthorised access to computer material; to gain unauthorised access to computer material with intent to commit or facilitate commission of further offences or to modify computer material without authorisation.

3. I understand that any hardware and software provided by my workplace for staff use can only be used by members of staff and only for educational use. To prevent unauthorised access to systems or personal data, I will not leave any information system unattended without first logging out or locking my login as appropriate.

4. I will respect system security and I will not disclose any password or security information. I will use a 'strong' password (A strong password has numbers, letters and symbols, with 8 or more characters, does not contain a dictionary word and is only used on one system and is changed regularly – every 28 days.

5. I will not attempt to install any purchased or downloaded software, including browser toolbars, or hardware without permission from the system manager.

6. I will ensure that any personal data of pupils, staff or parents/carers is kept in accordance with the Data Protection Act 2018. This means that all personal data will be obtained and processed fairly and lawfully, only kept for specific purposes, held no longer than necessary and will be kept private and secure with appropriate security measures in place, whether used in the workplace, hosted online (only within countries or sites with suitable data protection controls that meet the EU and UK regulations) or accessed remotely (e.g. via VPN). Any data which is being removed from the school site (such as via email or on memory sticks or CDs) will be encrypted by a method approved by the school). Any images or videos of pupils will only be used as stated in the school image use policy and will always take into account parental consent.

7. I will not keep or access professional documents which contain school-related sensitive or personal information (including images, files, videos, emails etc.) on any personal devices (such as laptops, digital cameras, mobile phones), unless they are suitably secured and encrypted. I will protect the devices in my care from unapproved access or theft.

8. I will not store any personal information on the school computer system including any school laptop or similar device issued to members of staff that is unrelated to school activities, such as personal photographs, files or financial information.

9. I will respect copyright and intellectual property rights.

10. I have read and understood the school online safety (e-Safety) policy which covers the requirements for safe ICT use, including using appropriate devices, safe use of social media websites and the supervision of pupils within the classroom and other working spaces

11. I will report all incidents of concern regarding children's online safety to the Designated Safeguarding Lead (Insert Name) and/or the Online Safety Coordinator (Insert Name) as soon as possible.

12. I will report any accidental access, receipt of inappropriate materials, filtering breaches or unsuitable websites to the Designated Safeguarding Lead and/or the Online Safety Coordinator (Insert Name) and/or the designated lead for filtering (Insert Name) as soon as possible.

13. I will not attempt to bypass any filtering and/or security systems put in place by the school. If I suspect a computer or system has been damaged or affected by a virus or other malware, or if I have lost any school related documents or files, then I will report this to the ICT Support Provider/Team/lead (Insert Name) as soon as possible.

14. My electronic communications with pupils, parents/carers and other professionals will only take place within clear and explicit professional boundaries and will be transparent and open to scrutiny at all times. All communication will take place via school approved communication channels e.g. via a school provided email address or telephone number and not via personal devices or communication channels e.g. personal email, social networking or mobile phones. Any pre-existing relationships or situations that may compromise this will be discussed with the Senior Leadership team and/or Head Teacher.

15. I will ensure that my online reputation and use of ICT and information systems are compatible with my professional role, whether using school or personal systems. This includes the use of email, text, social media/networking, gaming and any other devices or websites. I will take appropriate steps to protect myself online and will ensure that my use of ICT and internet will not undermine my professional role, interfere with my work duties and will be in accordance with the school AUP and the Law.

16. I will not create, transmit, display, publish or forward any material that is likely to harass, cause offence, inconvenience or needless anxiety to any other person, or anything which could bring my professional role, the school, or the Manchester City Council, into disrepute.

17. I will promote online safety with the pupils in my care and will help them to develop a responsible attitude to safety online, system use and to the content they access or create.

18. If I have any queries or questions regarding safe and professional practise online either in school or off site, then I will raise them with the Designated Safeguarding Lead and/or the Online Safety Coordinator or the Head Teacher.

19. I will only use my own log on the access school systems and will not share access with others.

20. I understand that my use of the school information systems (including any devices provided by the school), school Internet and school email may be monitored and recorded to ensure the safety of children and staff and to ensure policy compliance. This monitoring will be proportionate and will take place in accordance with data protection, privacy and human rights legislation.

*The School may exercise its right to monitor the use of information systems, including Internet access and the interception of emails in order to monitor policy compliance. Where it believes unauthorised and/or inappropriate use of the schools' information system or unacceptable or inappropriate behaviour may be taking place, the School will invoke its disciplinary procedure. If the school suspects that the school system may be being used for criminal purposes then the matter will be brought to the attention of the relevant law enforcement organisation.*

**I have read and understood and agree to comply with the Staff Acceptable Use Policy.**

Signed: …….. Print Name: …… Date: ……

Accepted by: ……. Print Name: …….

**Supply Teacher / Visitor / Volunteer Acceptable Use Policy**

***As a professional organisation with responsibility for children's safeguarding it is important that all members of the community are fully aware of their professional responsibilities and read and sign this Acceptable Use Policy. This is not an exhaustive list and visitors/volunteers are reminded that ICT use should be consistent with the school ethos, other appropriate school policies, relevant national and local guidance and expectations, and the Law.***

1. I will ensure that any personal data of pupils, staff or parents/carers is kept in accordance with the Data Protection Act 2018. Any data which is being removed from the school site (such as via email or on memory sticks or CDs) will be encrypted by a method approved by the school. Any images or videos of pupils will only be used as stated in the school image use policy and will always take into account parental consent.

2. I have read and understood the school online safety (e-Safety) policy which covers the requirements for safe ICT use, including using appropriate devices, safe use of social media websites and the supervision of pupils within the classroom and other working spaces.

3. I will follow the school's policy regarding confidentially, data protection and use of images and will abide with copyright and intellectual property rights, child protection legislation, privacy and data protection law and other relevant civil and criminal legislation.

4. My electronic communications with pupils, parents/carers and other professionals will only take place within clear and explicit professional boundaries and will be transparent and open to scrutiny at all times. All communication will take place via school approved communication channels e.g. via a school provided email address or telephone number and not via personal devices or communication channels e.g. personal email, social networking or mobile phones. Any pre-existing relationships or situations that may compromise this will be discussed with the Senior Leadership team and/or Head Teacher.

5. My use of ICT and information systems will be compatible with my role within school. This includes the use of email, text, social media, social networking, gaming, web publications and any other devices or websites. I will take appropriate steps to protect myself online and my use of ICT will not interfere with my work duties and will always be in accordance with the school AUP and the Law

6. I will not create, transmit, display, publish or forward any material that is likely to harass, cause offence, inconvenience or needless anxiety to any other person, or anything which could bring my professional role, the school, or the County Council, into disrepute.

7. I will promote online safety with the children in my care and will help them to develop a responsible attitude to safety online, system use and to the content they access or create.

8. If I have any queries or questions regarding safe and professional practise online either in school or off site, then I will raise them with the Designated Safeguarding Lead (Insert Name) or the Head Teacher.

9. I will report any incidents of concern regarding children's online safety to the Designated Safeguarding Lead (Insert Name) as soon as possible.

**I have read and understood and agree to comply with the Supply Teacher/ Visitor / Volunteer Acceptable Use Policy.**

Signed: …….. Print Name: …… Date: ……..

Accepted by:…… ……Date: ……..

**Wi-Fi Acceptable Use Policy For those using school Wi-Fi**

*As a professional organisation with responsibility for children's safeguarding it is important that all members of the school community are fully aware of the schools' boundaries and requirements when using the school Wi-Fi systems, and take all possible and necessary measures to protect data and information systems from infection, unauthorised access, damage, loss, abuse and theft. This is not an exhaustive list and all members of the school community are reminded that ICT use should be consistent with the school ethos, other appropriate policies and the Law.*

Please be aware that the school will not be liable for any damages or claims of any kind arising from the use of the wireless service. The School takes no responsibility for the security, safety, theft, insurance and ownership of any device used within the School premises that is not the property of the School.

The school provides Wi-Fi for the school community and allows access for education and school business use only. Wi-Fi passwords are only made available to the school network manager and School business manager.

1. The use of ICT devices falls under schools Acceptable Use Policy, online safety (e-Safety) policy and behaviour policy, data security, safeguarding/child protection, which all students/staff/visitors and volunteers must agree to, and comply with.

2. The school reserves the right to limit the bandwidth of the wireless service, as necessary, to ensure network reliability and fair sharing of network resources for all users.

3. School owned information systems, including Wi-Fi, must be used lawfully and I understand that the Computer Misuse Act 1990 makes the following criminal offences: to gain unauthorised access to computer material; to gain unauthorised access to computer material with intent to commit or facilitate commission of further offences or to modify computer material without authorisation.

4. I will take all practical steps necessary to make sure that any equipment connected to the schools' service is adequately secure (such as up-to-date anti-virus software, systems updates).

5. The school's wireless service is not secure, and the school cannot guarantee the safety of traffic across it. Use of the school's wireless service is done at my own risk. By using this service, I acknowledge that security errors and hacking are an inherent risk associated with any wireless network. For that reason, I expressly agree that I knowingly assume such risk, and further agree to hold the school harmless from any claim or loss arising out of, or related to, any such instance of hacking or other unauthorized use or access into my computer or device.

6. The school accepts no responsibility for any software downloaded and/or installed, e-mail opened, or sites accessed via the school's wireless service's connection to the Internet. Any damage done to equipment for any reason including, but not limited to, viruses, identity theft, spyware, plug-ins or other Internet-borne programs is my sole responsibility; and I indemnify and hold harmless the school from any such damage.

7. The school accepts no responsibility regarding the ability of equipment, owned by myself, to connect to the school's wireless service.

8. I will respect system security and I will not disclose any password or security information that is given to me. To prevent unauthorised access to systems or personal data, I will not leave any information system unattended without first logging out or locking my login as appropriate.

9. I will not attempt to bypass any of the schools' security and filtering systems or download any unauthorised software or applications.

10. My use of the school Wi-Fi will be safe and responsible and will always be in accordance with the school AUP and the Law including copyright and intellectual property rights. This includes the use of email, text, social media, social networking, gaming, web publications and any other devices or websites.

11. I will not upload, download, access or forward any material which is illegal or inappropriate or may cause harm, distress or offence to any other person, or anything which could bring the school into disrepute.

12. I will report any online safety (e-Safety) concerns, filtering breaches or receipt of inappropriate materials to the Designated Safeguarding Lead (Insert Name), the Online Safety (e-Safety) Coordinator (Insert Name) and/or the designated lead for filtering (Insert Name) as soon as possible.

13. If I have any queries or questions regarding safe behaviour online then I will discuss them with the Online safety (e-Safety) Coordinator (Insert Name) or the Head Teacher.

14. I understand that my use of the schools Wi-Fi will be monitored and recorded to ensure policy compliance in accordance with privacy and data protection legislation. If the schools' suspects that unauthorised and/or inappropriate use or unacceptable or inappropriate behaviour may be taking place, then the school terminate or restrict usage. If the School suspects that the system may be being used for criminal purposes then the matter will be brought to the attention of the relevant law enforcement organisation.

**I have read and understood and agree to comply with Hope School and College Wi-Fi Acceptable Use Policy.**

Signed: …….. Print Name: …… Date: ……

Accepted by: ……. Print Name: …….

**School Community Social Networking Acceptable Use Policy**

**For use with a member of the community running official online sites**

1. As part of the school's drive to encourage safe and appropriate behaviour in the use of today's technology, I will support the school's approach to online safety (e-Safety). I am aware that school websites, Twitter Facebook etc are a public and global communication tool/s and that any content posted on the site/page/group may reflect on the school, its reputation and services. I will not use the site/page/group to express any personal opinions or create, transmit, display, publish or forward any material that is likely to harass, cause offence, inconvenience or needless anxiety to any other person, or anything which could bring the school into disrepute.

2. I will not disclose information, make commitments or engage in activities on behalf of the school without authorisation from the school Designated Safeguarding Lead/ the head teacher. The head teacher (or other appropriate member of senior leadership) retains the right to remove or approve content posted on behalf of the school. Where it believes unauthorised and/or inappropriate use of the above tool/s or unacceptable or inappropriate behaviour may be taking place, the school will exercise the right to ask for the content to be deleted or deactivated.

3. I will ensure that any content posted abides by copyright and intellectual property rights, child protection legislation, privacy and data protection law and other relevant civil and criminal legislation.

4. I will follow the school's policy regarding confidentially and data protection/use of images. I will ensure that I have written permission from parents/carers or the school before using any images or videos which include members of the school community. Images of pupils will be taken on school equipment by the school and in accordance with the school image policy. Images which include pupils will only be uploaded by the school and these will be for the sole purpose of inclusion on the above tool/s and will not be forwarded to any other person or organisation.

5. I will promote online safety in the use of the above tool/s and will help to develop a responsible attitude to safety online and to the content that is accessed or created.

6. I will set up a specific account/profile using a school provided email address to administrate the site and I will use a strong password to secure the account. The school Designated Safeguarding Lead and school management team will have full admin rights to the account.

7. I will ensure that the content and channel is suitable for the audience and will be sensitive in the tone of language used and will ensure content is written in accessible plain English.

8. I will report any accidental access or receipt of inappropriate materials or inappropriate comments to the Designated Safeguarding Lead (Insert Name) and/or head teacher immediately.

9. I will ensure that the tool used is moderated on a regular basis as agreed with the Designated Safeguarding Lead (Insert Name) and/or head teacher.

10. I have read and understood the school online safety (e-Safety) policy which covers the requirements for safe ICT use, including using appropriate devices and the safe use of social media. I have ensured that the site has been suitably risk assessed and this use has been agreed by the head teacher.

11. If I have any queries or questions regarding safe and acceptable practise online, I will raise them with the Designated Safeguarding Lead (Insert Name) or the head teacher.

I have read and understood and agree to comply with the School Community Social Networking Acceptable Use policy.

Signed: …….. Print Name: …… Date: ……

Accepted by: ……. Print Name: …….

**Staff Social Networking Acceptable Use Policy**

*For use with staff running official school social media accounts*

1. As part of the school's drive to encourage safe and appropriate behaviour in the use of today's technology, I will support the school's approach to Online safety (e-Safety). I am aware that the tool a public and global communication tool and that any content posted may reflect on the school, its reputation and services. I will not use the site/page/group to express any personal opinions or create, transmit, display, publish or forward any material that is likely to harass, cause offence, inconvenience or needless anxiety to any other person, or anything which could bring the school into disrepute.

2. I will not disclose information, make commitments or engage in activities on behalf of the school without authorisation from the school Designated Safeguarding Lead (Insert Name) and/or the head teacher. The head teacher retains the right to remove or approve content posted on behalf of the school.

3. I will ensure that any content posted abides by copyright and intellectual property rights, child protection legislation, privacy and data protection law and other relevant civil and criminal legislation.

4. I will follow the school's policy regarding confidentiality and data protection/use of images. This means I will ensure that the school has written permission from parents/carers before using images or videos which include any members of the school community. Any images of pupils will be taken on school equipment, by the school and in accordance with the school image policy. Images which include pupils will only be uploaded by the school. These will be for the sole purpose of inclusion on tool used and will not be forwarded to any other person or organisation.

5. I will promote online safety (e-Safety) in the use of tool used and will help to develop a responsible attitude to safety online and to the content that is accessed or created. I will ensure that the communication has been appropriately risk assessed and approved by a member of senior leadership team/ Designated Safeguarding Lead/head teacher prior to use.

6. I will set up a specific account/profile using a school provided email address to administrate the account/site/page and I will use a strong password to secure the account. Personal social networking accounts or email addresses are not to be used. The school Designated Safeguarding Lead and/or school leadership team/head teacher will have full admin rights to the site/page/group.

7. Where it believes unauthorised and/or inappropriate use of the tool used e.g. Facebook, Twitter or unacceptable or inappropriate behaviour may be taking place, the school will exercise the right to ask for the content to be deleted or deactivated.

8. I will ensure that the content and channel is suitable for the audience and will be sensitive in the tone of language used and will ensure content is written in accessible plain English.

9. I will report any accidental access or receipt of inappropriate materials or inappropriate comments to the head teacher and/or Designated Safeguarding Lead urgently.

10. I will ensure that the site/page is moderated on a regular basis as agreed with the school Designated Safeguarding Lead.

11. I have read and understood the school online safety (e-Safety) policy which covers the requirements for safe ICT use, including using appropriate devices and the safe use of social media. I have ensured that the site has been suitably risk assessed and this use has been agreed by the head teacher.

12. If I have any queries or questions regarding safe and acceptable practise online, I will raise them with the Designated Safeguarding Lead (Insert Name) or the head teacher.

I have read and understood and agree to comply with the School Social Networking Acceptable Use policy.

Signed: …….. Print Name: …… Date: ……

Accepted by: ……. Print Name: ……

I will be managing the following official account:

School website

Year group Twitter account

Sports Twitter account

Other account

Details are as follows