HILLSIDE
HIGH SCHOOL

EXCELLENCE IN THE HEART
OF THE COMMUNITY

Online Safety Policy

2026-2027

Version Number: 01

Ratified by Local Governing Body: June 2026

Next Review Date: June 2027

School Link: A Jones

Contents:

1. Introduction..... 2
2. Roles and responsibilities..... 3
3. Child Protection..... 3
4. Online Safety & Safeguarding..... 4
5. Prevent..... 5
6. Remote Learning..... 6
7. Password Security..... 6
8. Data and Security..... 7
9. Managing the Internet..... 7
10. Infrastructure..... 8
11. Managing Email..... 8
12. Managing Other Web 2 Technologies..... 9
13. Mobile Technologies..... 9
14. Personal Mobile Devices (including phones) 10
15. School Provided Devices (including phones) 10
16. Taking of Images and Film..... 10
17. Publishing Pupils' Images and Work..... 11
18. Storage of Images..... 11
19. Webcams and CCTV..... 11
20. Complaints..... 11
21. Inappropriate Material..... 12

Appendix 1 – Staff Acceptable Use Agreement..... 13

Appendix 2 – Acceptable Use Agreement for Pupils..... 14

1. Introduction

1.1 ICT in the 21st Century is seen as an essential resource to support learning and teaching, as well as playing an important role in the everyday lives of children, young people and adults. Consequently, schools need to build in the use of these technologies in order to arm our young people with the skills to access life-long learning and employment.

1.2 Information and Communications Technology covers a wide range of resources including; web-based and mobile learning. It is also important to recognise the constant and fast paced evolution of ICT within our society as a whole. Currently the Internet technologies children and young people are using both inside and outside of the classroom include:

1.2.1 Websites.
1.2.2 Learning Platforms and Virtual Learning Environments.
1.2.3 Email and Instant Messaging.
1.2.4 Chat Rooms and Social Networking.
1.2.5 Blogs and Wikis.
1.2.6 Podcasting.
1.2.7 Video Broadcasting.
1.2.8 Music Downloading.

1.2.9 Gaming.

1.2.10 Mobile / Smart phones with text, video and / or web functionality.

1.2.11 Other mobile devices with web functionality.

1.3 Whilst exciting and beneficial both in and out of the context of education, much ICT, particularly web-based resources, are not consistently policed. All users need to be aware of the range of risks associated with the use of these Internet technologies.

1.4 We understand the responsibility to educate our pupils on online safety issues; teaching them the appropriate behaviours and critical thinking skills to enable them to remain both safe and legal when using the internet and related technologies, in and beyond the context of the classroom.

1.5 Both this policy and the Acceptable Use Agreement (for all staff, governors, visitors and pupils) are inclusive of both fixed and mobile internet; technologies provided by the school (such as PCs, laptops, personal digital assistants (PDAs), tablets, webcams, whiteboards, voting systems, digital video equipment, etc.) and technologies owned by pupils and staff, but brought onto school premises (such as laptops, mobile phones, camera phones, PDAs and portable media players, etc...).

1.6 This policy should be read alongside the following policies: Child Protection Policy, Behaviour for Learning Policy and Mobile Phone Policy and AI Policy

2 Roles and Responsibilities:

2.1 As online safety is an important aspect of strategic leadership within the school, the Executive Principal and Governors have ultimate responsibility to ensure that the policy and practices are embedded and monitored. For the purposes of this document the following staff are referenced throughout:

2.1.1 Executive Principal: Julia Anderson-Nicholls.

2.1.2 Designated Safeguarding Lead: Alanna Jones.

2.1.3 Designated Safeguarding Leads: Carla Sheils, Anne McGing.

2.1.4 Deputy Designated Safeguarding Leads: Wendy Banks, Ted Smedley.

2.1.5 ICT Network Technician: William Thomas.

2.2 All members of the school community have been made aware of who holds these posts. It is the role of the Designated Safeguarding Lead to keep abreast of current issues and guidance through organisations such as Sefton LA, CEOP (Child Exploitation and Online Protection) and Childnet.

2.3 Senior Leaders and Governors are updated by the Designated Safeguarding Lead and all Governors have an understanding of the issues and strategies at our school in relation to local and national guidelines and advice. This policy, supported by the school's Acceptable Use Agreement (for staff, governors, visitors), is to protect the interests and safety of the whole school community.

3 Child Protection

3.1 Members of The Safeguarding Team have completed relevant online safety training and are aware of the potential for child protection/safeguarding issues to arise from pupils' use of technology. Potential issues may include:

3.1.1 Sharing of personal data.
3.1.2 Access to illegal/inappropriate materials.
3.1.3 Inappropriate on-line contact with adults/strangers.
3.1.4 Sharing of nudes & semi-nudes.
3.1.5 Child on Child abuse/Sexual Violence & Sexual Harassment.
3.1.6 Potential or actual incidents of grooming/exploitation.
3.1.7 Bullying.
3.1.8 Terrorism and extremism material.

4 Online Safety & Safeguarding

4.1 All staff agree to the School's Acceptable Use Agreement (Appendix 1) and any new staff receive information on the school's Acceptable use Agreement as part of their induction.

4.2 All staff have been made aware of individual responsibilities relating to the safeguarding of children within the context of online safety and know what to do in the event of misuse of technology by any member of the school community.

4.3 All staff incorporate online safety activities and awareness within their curriculum areas. This is also taught through the school's Personal Development programme as well as through pastoral messages and assemblies. Pupils digitally sign to say they have read the Acceptable Use Agreement (Appendix 2). We ask that parents agree to support and uphold the principles of the Acceptable Use Policy in relation to their child's use of the Internet, at home and at school. We also ask parents/guardians to uphold the principles of this policy in relation to their own use of the Internet, when the use is related to school, employees of the school and other pupils at the school.

4.4 At Key Stage 3, online safety is taught through the Computer Science curriculum and the personal development curriculum. In teaching pupils about online safety, the school uses the DFE's guidance on how to stay safe online: Teaching online safety in school (January 2023) which has a focus on the following areas:

4.4.1 Knowledge and behaviours.
4.4.2 Harms and risks.
4.4.3 Navigating the Internet and managing information.
4.4.4 How to stay safe online.
4.4.5 Well-being.

4.5 The teaching of online safety also refers to key content in Keeping Children Safe in Education (2025) given that the use of technology has become a significant component of many safeguarding issues.

4.6 School has a duty to protect pupils from all forms of online harm including: online abuse; bullying or harassment; threats; impersonation; unwanted sexual advances; violent content; self-harm or suicide content and pornographic content. Please see Paragraph 4.8 for further details on the 4Cs.

4.7 It is essential that children are safeguarded from potentially harmful and inappropriate online material. The school has a duty to protect and educate pupils, and staff in their use of technology and establish mechanisms to identify, intervene in, and escalate any concerns where appropriate.

4.8 The breadth of issues classified within online safety is considerable but can be categorised into four areas of risks: Content, Contact, Conduct and Commerce. Hillside High School ensures that online safety is a running and interrelated theme whilst devising and implementing policies and procedures. This will include considering how online safety is reflected in all relevant polices and considering online safety whilst planning the curriculum, any teacher training, the role and responsibilities of the Designated Safeguarding Lead and any parental engagement.

4.8.1 **Content**: being exposed to illegal, inappropriate, or harmful content, for example: pornography, fake news, racism, misogyny, misandry, self-harm, suicide, anti-Semitism, Islamophobia, radicalisation, and extremism.

4.8.2 **Contact**: being subjected to harmful online interaction with other users; for example: peer to peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes.

4.8.3 **Conduct**: online behaviour that increases the likelihood of, or causes, harm; for example, making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography), sharing other explicit images and online bullying, and

4.8.4 **Commerce**: risks such as online gambling, inappropriate advertising, phishing and or financial scams.

4.9 The school also has clear procedures in place on the use of mobile and smart technology. Amongst other things this will reflect the fact many children have unlimited and unrestricted access to the internet via mobile phone networks (i.e. 3G, 4G and SG). This access means some children, whilst at school or college, could sexually harass other children via their mobile and smart technology, share indecent images consensually and non-consensually (often via large chat groups) and view and share pornography and other harmful content. Hillside High School carefully manages this through its Mobile Phone Policy and ensures this is reflected in procedures and our Child Protection & Safeguarding policy.

4.10 The school's website has a dedicated page for Parents/Guardians with advice on how to keep children safe online. This is regularly updated with advice to parents about Internet safety. Guidance for parents and updates are also sent via school newsletters.

4.11 To ensure pupils are safe online, the school has an enhanced monitoring and filtering system called Smoothwall. Smoothwall will detect any concerning words which are typed on a school computer linked to the harms specified in Paragraph 4.6 as well as inappropriate or concerning searches, images, uploads or downloads. School systems are monitored 24/7 and 365 days a year by Smoothwall and any concerning or offensive words, searches, images, uploads or downloads (even if deleted immediately) will trigger a response. Smoothwall will contact the Safeguarding Team, either by email or telephone (in case of emergency) and inform the school of the username of the pupil who the concern is related to.

4.12 When the Safeguarding Team receive an alert, a member of the team will speak to the pupil about the information received. Where necessary, parents/guardians will be informed and the information logged on CPOMs using the suitable category. Depending on the information received, appropriate support will be offered. Incidents of inappropriate use will be dealt

with in line with other school policies such as: Behaviour for Learning, Safeguarding & Child Protection and Anti-Bullying.

4.13 The purpose of Smoothwall is not to invade a pupil's privacy but to ensure that everyone in school is safeguarded and can receive the right support if and when needed. It is also to ensure that school can effectively deal with potential bullying or abuse and is in line with the school's Acceptable Use Policy which all pupils are required to sign.

5 Prevent

5.1 Under duties imposed within the Prevent Duty Guidance 2023 as part of the Counterterrorism and Security Act 2015, Hillside High School will ensure that situations are suitably risk assessed, that they will work in partnership with other agencies, that all staff are suitably trained and that IT policies will ensure that children and young people are safe from terrorist and extremist material when accessing the Internet in school.

5.2 The School Lead (Single Point for Contact) for Prevent is: Alanna Jones. The SPOC will link with other relevant agencies (including the Police) to ensure that vulnerable people are appropriately supported and risk assessed, and that staff and Governors are trained to an appropriate level to ensure they are able to recognise any concerns. The specific Roles and Responsibilities of this Single Point of Contact (SPOC) are defined in the school's Child Protection Policy.

6 Remote Learning

6.1 There may be occasions where the school will need to implement a 'remote learning' approach to education. This might be due to health reasons or when extreme weather prevents the school from fully opening.

6.2 It is important that all staff who interact with children, including online, continue to look out for signs a child may be at risk. Any such concerns should be dealt with as per the Child Protection Policy and where appropriate referrals should still be made to Children's Social Care (iCART) and as required, the police.

6.3 Online teaching should follow the same principles as set out in the school's Code of Conduct and in line with Guidance for Safer Working Practice. Below are some factors to consider if there are virtual lessons, especially where webcams are involved:

6.3.1 No 1:1s; groups only unless this has been agreed.

6.3.2 Staff and children must wear suitable clothing, as should anyone else in the household.

6.3.3 Any computers used should be in appropriate areas, for example, not in bedrooms and the background should be blurred.

6.3.4 Live classes should be kept to a reasonable length of time, or the streaming may prevent the family 'getting on' with their day.

6.3.5 Language must be professional and appropriate, including any family members in the background.

6.3.6 Staff must only use platforms specified by senior managers and approved by our IT network manager/provider to communicate with pupils.

6.3.7 Staff should record the length, time, date and attendance of any sessions held.

7 Password Security

7.1 Password security is essential for staff, particularly as they are able to access and use pupil data. Staff are expected to have secure passwords which are not shared with anyone. Staff are regularly reminded of the need for password security. Staff are required to set their own password that meets the security requirements set out by Mr Thomas, IT Technician. Staff must regularly change passwords and ensure they are not shared.

7.2 If staff believe their password may have been compromised or someone else has become aware of their password, they must report this to Mr Thomas, IT Technician.

7.3 Staff are made aware of their individual responsibilities to protect the security and confidentiality of school networks, MIS systems and/or Learning Platform.

7.4 All users must make sure that workstations are not left unattended and are locked.

7.5 In school, all IT password policies are the responsibility of the System Manager and all staff are expected to comply with the policies at all times.

8 Data and Security

8.1 The accessing and appropriate use of school data is something that the school takes very seriously. The school follows the Information Commissioners Office (ICO) guidelines:

8.1.1 Staff are made aware of their responsibility when accessing school data.

8.1.2 The Level of access is determined by either the Executive Principal and/or the IT Network Manager.

8.1.3 Confidential or sensitive data taken off the school premises must be encrypted.

8.1.4 Data can only be accessed and used on school computers or laptops. Staff are aware they must not use their personal devices for accessing any confidential or sensitive data without the express permissions of the Executive Principal.

8.1.5 Only software properly purchased and/or approved by IT Support may be used on the school's hardware. It is the responsibility of the user to ensure that IT Support is fully consulted if they wish to install additional software on their laptop. It is also the responsibility of the user to ensure that any licensing issues are addressed promptly.

8.1.6 It is policy to store data on a network drive which is backed up each day. It is the responsibility of each individual user to ensure that data not stored on the network is backed up regularly. The school does not take responsibility for data not in the backup plan being lost, deleted stolen etc...

8.1.7 Personal devices (Laptops, Mobile Phones etc...) are not permitted to be used on the system or connected to the wireless infrastructure without the express permissions of the Executive Principal and/or IT Network Manager.

8.1.8 The school does not guarantee the security of any information users may enter while making permitted personal use of a school computer. The school disclaims all liability that may arise from loss or harm suffered by a user as a result of that information being disclosed to or obtained by any other person and then being further disclosed or being used so as to cause loss to the user. The school disclaims

all liability for such losses and any employee using a school computer for permitted private purposes does so on the basis of having agreed this disclaimer of liability.

8.1.9 Staff using personal removable media are responsible for measures to protect against viruses, for example making sure that additional systems used have up-to-date virus protection software. It is neither the school's responsibility nor the IT Technician's to install or maintain virus protection on personal systems.

8.1.10 If there are any issues related to viruses or anti-virus software, the IT Technician immediately should be informed.

9 Managing the Internet

9.1 The internet is an open communication medium, available to all, at all times. Anyone can view information, send messages, discuss ideas and publish material which makes it both an invaluable resource for education, business and social interaction, as well as a potential risk to young and vulnerable people. All use of the Internet is logged and the logs are randomly but regularly monitored. Whenever any inappropriate use is detected, it will be followed up.

9.2 All users must observe software copyright at all times. It is illegal to copy or distribute school software, non-licensed software or illegal software. All users must observe copyright of materials from electronic resources.

9.3 Staff will preview any recommended sites before use. Raw image searches are discouraged when working with pupils. If Internet research is set for homework, specific sites will be suggested that have previously been checked by the teacher. It is advised that parents/guardians recheck these sites and supervise this work. Parents/guardians will be advised to supervise any further research.

10 Infrastructure

10.1 School Internet access is controlled through the IBoss web filtering software with a bought in whitelist solution.

10.2 Hillside High School is aware of its responsibility when monitoring staff communication under current legislation and takes into account; Data Protection Act 2018/GDPR, The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, Regulation of Investigatory Powers Act 2000, Human Rights Act 1998.

10.3 The school ensures children are safe from terrorist and extremist material when accessing the Internet in school, including by establishing appropriate levels of filtering in accordance with the Prevent Duty Guidance 2015.

10.4 Staff are aware that school Internet activity can be monitored and explored further if required. Intrusions into the privacy of employees must be proportionate to the purpose of the monitoring.

10.5 The school uses a tutor management control tools for controlling and monitoring workstations. If staff discover an unsuitable site, the incident must be reported immediately to the IT Technician or the Safeguarding Team.

10.6 It is the responsibility of the school, by delegation to the IT Technician, to ensure that Anti-virus protection is installed and kept up-to-date on all school machines.

10.7 Staff are not permitted to download programs on school-based technologies without seeking prior permission from IT Support.

11 Managing Email

11.1 The use of email within most schools is an essential means of communication for both staff and pupils. In the context of school, email should not be considered private. Educationally, email can offer significant benefits including direct written contact between schools on different projects, be they staff based or pupil based, within school or international.

11.2 The school gives all staff their own email account to use for all school business. This is to minimise the risk of receiving unsolicited or malicious emails and avoids the risk of personal profile information being revealed. It is the responsibility of each account holder to keep their password secure. For the safety and security of users and recipients, all mail is filtered and logged; if necessary, email histories can be traced. This should be the account that is used for all school business. Under no circumstances should staff contact pupils, parents or conduct any school business using personal email addresses.

11.3 Email sent to an external organisation should be written carefully before sending, in the same way as a letter written on school headed paper. Staff sending emails to external organisations, parents/guardians or pupils are advised to cc. their Line Manager. **The forwarding of chain emails is not permitted in school.** All email users are expected to adhere to the generally accepted rules of network etiquette (netiquette) particularly in relation to the use of appropriate language and not revealing any personal details about themselves or others in email communication. Pupils' initials are recommended to be used in correspondence rather than the full name.

11.4 Staff must inform their line manager if they receive an offensive email.

11.5 The School will assist the relevant authorities in taking action against any employee who commits an unlawful act whilst using the School's computer facilities. The School will report criminal activity to the Police.

11.6 Personal or business emails, whether created or stored on School equipment, constitute a School record and as such are deemed to be property of the School.

11.7 Emails from unknown sources or which may appear suspicious must not be opened. Software received via email must not be installed. You must consult IT Technician for advice if you receive software via email or email from an unknown source or which is otherwise suspicious.

11.8 **Emails are formal documents and must not contain remarks that might be potentially embarrassing to the School, its employees, the Trust or the general public.**

12 Managing Other Web 2 Technologies

12.1 Web 2, including social networking sites, if used responsibly both outside and within an educational context can provide easy to use, creative, collaborative and free facilities. However, it is important to recognise that there are issues regarding the appropriateness of some content, contact, culture and commercialism.

12.2 At present, the school allows access to social networking sites for Staff within school; this allows for better connectivity with a range of online learning technologies.

12.3 School staff with social networking profiles should ensure that they set the privacy levels on their accounts to the maximum i.e. only people on their 'friends or trusted' lists should be able to view their pictures/private information.

12.4 The school specifies the following guidelines should a message from a pupil be received:

12.4.1 Do not reply to the message. Replying to a message allows the recipient to view your profile in its entirety. This is also a way to circumvent the privacy settings on accounts.

12.4.2 Inform the school's Designated Safeguarding Lead at the earliest opportunity and advise them of the full details of the incident. The relevant communication should be made available to the member of staff to aid in any investigation.

12.5 The School advises staff to keep their account privacy as high as possible. Any contact from a pupil, or attempted contact, must be immediately reported to the school Designated Safeguarding Lead. Staff should not respond to any contact/request for contact from any pupil other than to delete/block.

12.6 As a professional, you must remember that in addition to protecting yourself, you should not participate in anything via social media that would bring your employer into disrepute.

12.7 All staff are advised to be cautious about the information given by others on sites, for example users not being who they say they are.

12.8 Staff are encouraged to be wary about publishing specific and detailed private thoughts online. A general rule is don't post/share/tweet/re-tweet anything you would not be happy for your Executive Principal to see.

13 Mobile Technologies

13.1 Many emerging technologies offer new opportunities for teaching and learning including a move towards personalised learning and 1:1 device ownership for children and young people. Many existing mobile technologies such as portable media players, PDAs, gaming devices, mobile and Smart phones are familiar to children outside of school too. They often provide a collaborative, well-known device with possible internet access and thus open up risk and misuse associated with communication and Internet use. Emerging technologies will be examined for educational benefit and then risk assessed before use in school is allowed.

14 Personal Mobile Devices (including phones)

14.1 The school allows staff to bring in personal mobile phones and devices for their own use. Under no circumstances does the school allow a member of staff to contact a pupil using their personal device.

14.2 Staff are advised to always contact parents/guardians using the school's phone system. If a member of staff does need to contact a parent/guardian using their own device, personal numbers from devices should be blocked.

14.3 The school is not responsible for the loss, damage or theft of any personal mobile device.

14.4 The sending of inappropriate text messages between any members of the school community is not allowed.

14.5 Whilst on the premises or while conducting official school business, permission must be sought before any image or sound recordings are made on personal devices by any member of the school community.

14.6 Users bringing personal devices into school must ensure there is no inappropriate or illegal content on the device.

14.7 While in school, personal mobile phones shall be set on discreet mode.

14.8 Mobile phones shall only be used in work in accordance with instructions issued by the school's mobile phone guidelines.

15 School Provided Devices (including phones)

15.1 Where the school provides mobile technologies such as phones or laptops for offsite visits and trips, only these devices should be used to conduct school business.

15.2 Fixed telephony equipment must not be moved, unplugged or switched off except with the express permission of Mr Thomas, IT Technician.

15.3 Settings on telephones must not be altered as this could cause a failure to ring. Proper use of divert or follow me facilities is permitted.

15.4 Personal incoming calls (by landline or mobile) with the exception of emergencies whilst at work, should be discouraged and where unavoidable must be kept to a minimum.

16 Taking of Images and Film

16.1 Digital images are easy to capture, reproduce and publish and, therefore, misused. We must remember that it is not always appropriate to take or store images of any member of the school community or public, without first seeking consent and considering the appropriateness.

16.2 With the written consent of parents / guardians (on behalf of pupils) in the admission form, the school permits the appropriate taking of images by staff and pupils with school equipment.

16.3 Staff are not permitted to use personal digital equipment, such as mobile phones and cameras, to record images of pupils; this includes when on field trips. However, with the express permission of the Executive Principal, images can be taken provided they are transferred immediately and solely to the school's network and deleted from the staff device.

17 Publishing Pupils' Images and Work

17.1 On a child's entry to the school, all parents/guardians will be asked to give permission to use their child's work/photos in the following ways:

17.1.1 On the school website.

17.1.2 On the school's Twitter/Instagram pages/Social Media pages.

17.1.3 In the school prospectus and other printed publications that the school may produce for promotional purposes.

17.1.4 Recorded/transmitted on a video or webcam.

17.1.5 In display material that may be used in the school's communal areas.

17.1.6 In display material that may be used in external areas, i.e. exhibition promoting the school.

17.1.7 General media appearances, e.g. local/national media/press releases sent to the press highlighting an activity (sent using traditional methods or electronically).

17.2 This consent for this is gathered on pupils' admission form and is considered valid for the entire period that the child attends this school unless there is a change in the child's circumstances where consent could be an issue, e.g. divorce of parents, custody issues, etc.

17.3 Parents/guardians may withdraw permission, in writing, at any time.

17.4 Pupils' full names will not be published alongside their image and vice versa. Email and postal addresses of pupils will not be published.

17.5 Before posting pupil work or images external to the school, e.g. on the Internet or distributing to the Press, a check needs to be made to ensure that permission (from the parents/guardians and the pupil) has been given for work to be displayed. This is the responsibility of the member of staff submitting the information.

17.6 Pupil names should be shared in the format of first name and initial if sharing on social media or newsletters.

18 Storage of Images

18.1 Images/films of children are stored only on the school's network. Pupils and staff are not permitted to use personal portable media for storage of images (e.g. USB sticks) without the express permission of the Executive Principal. Rights of access to this material are restricted to the teaching staff and pupils within the confines of the school network/Learning Platform. Images must be deleted when they are no longer required.

19 Webcams and CCTV

19.1 The school uses CCTV for security and safety. Notification of CCTV use is displayed around the school site.

19.2 We do not use publicly accessible webcams in school. Webcams in school are only ever used for specific learning purposes. Consent is sought from parents/guardians and staff on joining the school, in the same way as for all images.

20 Complaints

20.1 Complaints relating to online safety should be made to Ms A. Jones, AVP in the first instance. They will then be referred to the school's Complaints Policy. All incidents should be logged.

21 Inappropriate Material

21.1 All users are aware of the procedures for reporting accidental access to inappropriate materials. The breach must be immediately reported to the IT Technician.

21.2 Deliberate access to inappropriate materials by any user will lead to the incident being logged by the IT Technician.

This policy will be reviewed annually. After every review, it will be approved by the Local Governing Body.

Appendix 1 - Staff Acceptable Use Agreement

This is the Acceptable Use Agreement for our school. The purpose of this policy is to promote positive and responsible network and Internet behaviour. Please read carefully; by acknowledging that you have read this policy, you will be indicating that you agree to the terms set out below. Staff will periodically (each term) be asked to digitally sign the AUA when they login into the school network.

Staff:

- I will only use school IT systems, external logins and email for school related purposes. Other use will be with the permission of SLT.
- I will not divulge any school related passwords and I will comply with school IT security procedures.
- I will make sure email with staff, parents, pupils and members of the public are responsible and in line with school policies.
- I will not give my home address, phone number, mobile number, personal social networking details or personal email address to pupils.
- I accept that pupils may find these details out, and that any contact should be logged and either not reciprocated or replied to in line with school policies. I should be responsible and aware of my professional responsibilities and school policies if I supply any personal details to parents.
- I will use school email systems for school related communications. I will not use personal accounts for school business.
- I will ensure that personal data is stored securely and in line with the Data Protection Act/GDPR. I will follow school policy with regard to external logins, encrypted data and not storing school material on personal IT equipment.
- I will not install software onto workstations or the network unless supervised by the Network Manager or IT support staff.
- I will not search for, view, download, upload or transmit any material which could be considered illegal, offensive, defamatory or copyright infringing using school IT equipment.
- Photographs of staff, pupils and any other members of the school community will not be used outside of the internal school IT network unless written permission has been granted by the subject of the photograph or their parent/guardian. I will ask the permission of the Executive Principal (on site) or the proprietor of the building (off site) prior to taking any photographs.
- I am aware that all network and Internet activity is logged and monitored and that the logs are available to SLT in the event of allegations of misconduct.
- I will not write or upload any defamatory, objectionable, copyright infringing or private material, including images and videos, of pupils, parents or staff on social media or websites in any way which might bring the school into disrepute.
- I will make sure that my Internet presence does not bring the teaching profession into disrepute and that I behave online in line with school policy.
- I will champion the school's e-safety policy and be a role model for positive and responsible behaviour on the school network and the Internet.
- I will not make comments about school on personal social media, whether positive or negative.
- I will not use my personal phone or camera to take photographs of pupils even if this is for a school purpose.

Appendix 2 - Acceptable Use Agreement for Pupils

This is the acceptable usage policy for our school. The purpose of this policy is to promote positive and responsible network and Internet behaviour. Please read carefully and click at the bottom to say that you agree. If you do not click and agree you will not be able to use the school's IT systems. Pupils will periodically (each term) be asked to digitally sign the AUA when they login into the school network.

Pupils:

- I will only use school Internet and IT facilities for educational purposes which follow the teachers' instructions. This includes email, video, messaging, video-conferencing, social media, Internet, file-saving and printing.
- I will not use my mobile phone in school (this includes checking time, checking messages, making phone calls) unless permission is granted. If permission is granted, I will use my mobile device as if it was a school computer, following all the rules for using school computers.
- I will not install software on school IT facilities due to the risk of damage being caused by malware or viruses. I will ask a teacher to install software if required.
- I will not share my network, Internet or any other school-related passwords.
- I will change my passwords when asked to.
- I will only use my school-supplied email address for school-related activities.
- I will not look at or delete other people's work or files.
- I will make sure all my contact with other people at school is responsible. I will not cyber-bully pupils or teachers.
- I will be responsible and polite when I talk online to pupils, teachers and other people related to the school, both in school-time and outside school-time.
- I won't look for or look at unpleasant or inappropriate websites in school. I will check with a teacher if I think a website might be unsuitable.
- I won't give out my personal details, such as my name, address, school or phone number on the Internet.
- I won't meet people I've met on the Internet unless I have told my parents and they come with me.
- I won't upload or download any pictures, writing or films which might upset people online.
- I won't write unpleasant, rude or untrue comments online about pupils, teachers or the school.
- I will treat all IT equipment at school with respect and ensure the computer is left in the state that I found it.
- I am aware that everything I do on the computers at school is monitored and logged, and that the school can talk to my parents if a teacher is concerned about my online safety or my behaviour when using school computers.
- I will respect copyright when making use of images and videos in my school work.
- I will not look for, view, upload or download offensive, extremist, illegal, copyright-infringing or pornographic material. If I find such material on school IT equipment I will inform a teacher immediately.
- Images of pupils will only be taken, stored and used for school purposes in line with school policy. Images will only be used on the Internet or in the media with permission.
- I am aware that the school uses an online monitoring and filtering system called Smoothwall to safeguard pupils.

- I am aware that Smoothwall will alert school if any concerning or offensive words, searches, images, uploads or downloads (even if deleted immediately) are accessed on school systems.
- I am aware that school will use the Smoothwall system to offer appropriate support but also to ensure that it can effectively deal with potential bullying or abuse. Such instances may be dealt with in line with the school's Behaviour for Learning Policy and the Anti-Bullying Policy.
- I will not look for ways to bypass the school filtering or proxy service or bypass the school filtering or proxy service.
- I understand that these rules are designed to keep me safe and that if they are not followed, sanctions may be applied and my parent/guardian may be contacted.

Full name: Form:

Signed: