Holte School

Online Safety Policy

Lead member of staff:	Lee Farmer (Assistant Headteacher, Pastoral)
Legislation Status: (Statutory/Non-Statutory)	Statutory
Local Authority Model Policy or School Written Policy:	School Written Policy
Required on school website:	Yes
Revision Date:	May 2023
Date Ratified By Full Governing Body:	June 2023
Signed By Chair Of Governors: **Ms C Hardy**	C Hardy

1. Rationale

1.1 With the increasing availability of devices which give unrestricted access to the internet for children, Holte School considers online safety to be extremely important. We endeavour to ensure that every student in Holte's care is safe; and the same principles apply to the digital world as apply to the real world. This policy applies to all Holte staff, volunteers, visitors, parents and students.

1.2 ICT and online communications provide unrivalled opportunities for enhanced learning in addition to traditional methods, but also pose greater and more subtle risks to young people. Holte School has a responsibility to provide a safe environment in which children can learn. Our students are therefore taught how to stay safe in the online environment and how to mitigate risks, including but not limited to the risk of identity theft, cyber-bullying, extremism, radicalisation, harassment, grooming, peer on peer abuse, sexual harassment and violence, gang activity including County Lines, stalking and abuse.

2. Aims and objectives

2.1 The aim of this policy is to establish the ground rules we have in school for using ICT equipment and the Internet. New technologies have become integral to the lives of children and young people in today's society, both within educational establishments and in their lives outside school.

2.2 The Internet and other digital/information technologies are powerful tools which open up new opportunities for everyone but there are risks attached to them. The same standards of behaviour are expected online as apply offline, and that everyone should be treated with kindness, respect and dignity. Some of the dangers our students may face include:

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

2.3 The breadth of issues classified within online safety is considerable, but can be categorised into four areas of risk as defined in Keeping Children Safe in Education:

- Content: being exposed to illegal and harmful content (e.g. pornography, extremist content).
- Contact: harmful interactions (e.g. grooming).
- Conduct: personal online behaviours (e.g. sending & receiving explicit images).
- Commerce: risks such as online gambling, inappropriate advertising, phishing and or financial scams

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

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

2.5 Online safety is a concern for everyone. Students, teachers and parents in the wider school community should all work collaboratively to prevent online bullying and to develop a safe and positive attitude towards technology and online engagement.

2.6 The school provides the necessary safeguards to help ensure that we have done everything that could reasonably be expected to manage and reduce these risks. The online safety policy explains how the school intends to do this, whilst also addressing wider educational issues in order to help young people (and their parents/carers/staff) to be responsible users and stay safe while using the Internet and other communications technologies for educational, personal and recreational use.

2.7 The UN Convention on the Rights of the child state that 'the best interests of the child must be a top priority in all decisions and actions that affect children.' Article 19 states that governors must do all they can to ensure that children are protected from all forms of violence, abuse, neglect and bad treatment by their parents or anyone else who looks after them.

Holte School is committed to the principles of the Convention and is actively committed in fulfilling its responsibilities as a Rights Respecting School.

3. Scope of the online safety policy

3.1 The School's online safety policy is in line with the following national frameworks:

- Teaching online safety in schools (DfE, June 2019)
- Behaviour in Schools Guidance (DfE, September 2022)
- Keeping children safe in education (September 2022)
- Ofsted Common Inspection Framework (October 2019)
- The Prevent duty (June 2015)
- Working together to safeguard children (March 2015)
- The Prevent Strategy (June 2011) and Channel guidance (April 2015)
- FGM mandatory reporting duty (October 2015)
- Education in a Connected World (February 2018)
- Sexual violence and sexual harassment between children in schools and colleges (May 2018)
- UK Safer Internet – Appropriate filtering and Monitoring

3.2 This policy has links to the following policies:

- Whole School Policy for Safeguarding and Child Protection
- Relationship and Behaviour Policy
- Citizenship & PSHE Policy
- Anti-bullying
- Professional Code of Conduct
- Acceptable Use of ICT including Social Media Policy
- Data Protection Policy

3.2 This policy applies to all members of the school community (including staff, pupils, governors, volunteers, parents/carers and visitors) who have access to and are users of school IT systems, both in and out of school. This policy, supported by the Acceptable Use Policy for all staff and students, is implemented to protect the interests and safety of the whole school community. It aims to provide clear guidance on how to minimise risks and how to deal with any infringements.

3.3 The Education and Inspections Act 2006 empowers Headteachers, to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying or other online safety incidents covered bythis policy, which may take place out of school, but is linked to membership of the school.

3.4 The school will deal with such incidents within this policy and in associated behaviour and anti-bullying policies and will, where known, inform parents/carers of incidents of inappropriate online safety behaviour that take place out of school.

4. Roles & Responsibilities

This section outlines the roles and responsibilities for online safety of individuals and groups within the school.

4.1 Governors

Governors are responsible for the approval of the online safety policy and for reviewing the effectiveness of the policy. A member of the Governing Body, Chris Hardy, is responsible for Safeguarding/Child Protection and online safety will be a part of this. The governing body receives annual training for Safeguarding/Child Protection and are aware of the relevant legislation with regards to online safety concerns. The Headteacher and governors are responsible for ensuring that appropriate filters and monitoring systems are in place. The governing body has read and understood Annex C of Keeping Children Safe in Education.

4.2 Headteacher

The Headteacher is responsible for ensuring the safety (including online safety) of all members of the school community, although the day to day responsibility for online safety is delegated to the Deputy Headteacher – Inclusion, Assistant Headteacher - Pastoral, ICT Network Manager, and the Head of ICT. The Headteacher and governors are responsible for ensuring that appropriate filters and monitoring systems are in place.

4.3 Designated Safeguarding Lead (DSL)

Online safety is a significant part of the responsibilities of the school's Designated Safeguarding Lead, (DSL). The DSL at Holte School is Andy Oliver. The DSL accesses regular training (e.g. e-bulletins, attendance at Police and Schools Panel) to ensure that they are able to understand the unique risks associated with online safety, including the additional risks that children with SEN and disabilities (SEND) face online. The DSL liaises with the SENCo to ensure that SEND students are effectively protected from such risks.

The DSL is supported in this role by the Assistant Headteacher – Pastoral, who is a CEOP Ambassador. This ensures that there is the relevant knowledge and capability required to keep all children safe when they are online. The DSL's responsibilities also includes the monitoring and filtering of the school's network in conjunction with the Headteacher.

The DSL follows the UKCCIS sexting guidance for schools and colleges when responding to sexting concerns and the DfE guidance, Sexual violence and sexual harassment between children in schools and colleges (May 2018).

4.4 Assistant Headteacher - Pastoral

The Assistant Headteacher - Pastoral takes day to day responsibility for online safety issues and has a leading role in:

- Liaising with staff, the DSL, LA, ICT Network Manager, Safeguarding Governor and SLT on all issues related to online safety, including Child Sexual Exploitation (CSE) extremism and radicalisation, and gang activity including County Lines;
- Ensuring that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place;
- Adequate training is provided for staff in online safety, including Child Sexual Exploitation and extremism and radicalisation;
- Adequate guidance and support for parents in online safety, including Child Sexual Exploitation and extremism and radicalisation;
- Effective recording and monitoring systems are set up and outcomes are rigorously analysed;
- Maintaining a reporting system (e.g. Whisper & ePraise) to provide pupils with an avenue to report concerns;
- Co-ordinating and reviewing an online safety education programme in school;
- That relevant procedures in the event of an online safety allegation are known and understood;
- Establishing and reviewing the school online safety policies and documents;
- The school's Designated Safeguarding Leads are trained in online safety issues and be aware of the potential for serious child protection issues to arise through the use of IT.

4.5 ICT Network Manager

The Network Manager is responsible for ensuring that:

- The school's ICT infrastructure is secure and meets online safety technical requirements;
- The school's password policy is adhered to;
- The school's filtering and monitoring system is applied and updated on a regular basis;
- The Network Manager keeps up to date with online safety technical information;
- The use of the school's ICT infrastructure (network, remote access, e-mail, VLE etc.) is regularly monitored in order that any misuse or attempted misuse can be reported to the Deputy Headteacher – Inclusion, and Assistant Headteacher-Pastoral for investigation, action and sanction.

4.6 Teaching & Support Staff

Safeguarding including online safety is the responsibility of all adults within the school. Teachers should be aware of the dangers and risks associated with the use of technology, including bullying, grooming, sexting, and radicalisation. They should also be aware of any publicly available online content that could pose a threat to or influence children, especially issues which are reported through the press.

All teaching and support staff are responsible for ensuring that:

- They provide a safe online environment for all students and know what to do if there is a disclosure from a student with respect to online safety, including an incident involving youth produced sexual imagery;
- They have an up-to-date awareness of online safety matters and of the current school online safety policy and practices through the completion of regular training, including Prevent training;
- They have an awareness of indicators of online safety abuse (including emotional e.g. peer-on-peer abuse or cyberbullying, and sexual abuse e.g. youth produced sexual imagery) and safeguarding issues relating to online safety.
- They have read, understood and signed the school acceptable use of ICT including social media agreement every year.
- Online safety issues are embedded in all aspects of the curriculum and other school activities, including the SMSC curriculum;
- Students understand and follow the school's online safety policy and follow the guidelines on acceptable internet use in their planners;
- They monitor ICT activity in lessons, extracurricular and extended school activities;
- In lessons where Internet use is pre-planned, pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in Internet searches.

4.7 Students

Digital literacy and citizenship should be included in a clear and progressive curriculum, to ensure that pupils understand how to conduct themselves online in a safe and appropriate manner. Children should enjoy learning about emotional health and relationships in both online and offline environments.

- Are responsible for using the school ICT systems in accordance with the guidance contained in their planners;
- All students are asked to sign in their planner an agreement pertaining to social media usage;

- Need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know that Whisper is available to allow them to do this;
- Should understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the school's online safety policy can also cover their actions out of school.

4.8 Parents/Carers

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

Parents and carers will be responsible for:

- Endorsing via signature the guidance in the pupil planner pertaining to social media and social networking;
- Attending advice sessions that Holte School provides for parents.

5. Education and Training

5.1 The breadth of issues classified within online safety is considerable but can be categorised into three areas of risk – Content, Contact, Conduct and Commerece. Digital literacy and online safety education engages all learners with these risks in in the following ways:

- The responsibility for teaching children about online safety is not the sole responsibility of the ICT curriculum; it is woven throughout the curriculum and across all age groups from Year 7 – 13.
- The school's curriculum for teaching students about online safety has been reviewed in light of the recommendations in 'Education for a Connected World' (February 2018), Keeping Children Safe in Education (September 2018) and Teaching Online Safety in Schools (June 2019). The curriculum is reviewed annually.
- In ICT lessons at Key Stage 3 students learn about age restrictions, cybersecurity, disinformation cyberbullying, Phishing, fake websites and scams, chatroom safety, texting and internet safety and the impact of social media on individuals and communities, personal data, unsafe communication, abuse, fake profiles,reputational damage and privacy settings.
- At Key Stage 4, (BTEC ICT) students learn about disinformation, cybersecurity, Phishing, fake websites and scams, Cyberbullying, Location - aware applications, Malware and Security, Hacking and Social media, personal data, and persuasive design.
- The ICT department model and promote online safety at every opportunity, particularly during Safer Internet Day. They use ABTutor to monitor student use of the Internet during lessons.
- Online safety advice is provided as part of the SMSC and assembly programme and is regularly revisited in lessons across the curriculum.
- Students are taught in lessons to be critically aware of the materials/content they access on-line and are guided to validate the accuracy of the information.
- Students are taught about 'fake news' and how to identify and respond to 'fake news' on the Internet.
- Students are encouraged to adopt safe and responsible use of ICT, the Internet and mobile devices both within and outside of school during Citizenship/PSHE sessions.
- Students are taught about online safety in the context of extremism and radicalisation, gang activity including County Lines and Child Sexual Exploitation through Citizenship and PSHE activities.
- Online safety is a significant part of the school's Relationship, Sex and Health Education (RSHE) curriculum. For example, lessons cover topics such as pornography, grooming, live streaming, suicide, self-harm and eating disorders.

- Students are taught about the role of technology within peer-on-peer abuse and online harassment.
- Rules for the use of ICT systems and the Internet are in all student planners.
- Staff act as good role models in their use of ICT, the Internet and mobile devices.
- Students receive a weekly safeguarding bulletin that includes important information and support on online safety.
- Emerging technologies will be examined for educational benefit and a riskassessment will be carried out before use in school is allowed.
- The school may use external agencies to complement and reinforce the school's online safety curriculum. External agencies cannot be used without the authorisationof the DSL and a review of the content delivered.
- Students have an opportunity to train as Childnet digital leaders. Digital leaders will lead training for their peers and parents throughout the academic year and will help the school in raising the profile of online safety. Digital leaders will support the ICT department in the annual review of how online safety is addressed within the curriculum.

5.2 Staff Training

- The school will ensure that all staff receive appropriate, annual and up to date training regarding online safety. This may be led by the school's CEOP Ambassadors or using the National College. It is made clear to all staff that online safety is a matter of professional practice as well as safeguarding children.
- The school will ensure that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place.
- The Assistant Headteacher – Pastoral is a CEOP trained Ambassador and DSL and is responsible for coordinating the training of all staff on issues relating to online safety in conjunction with the Designated Safeguarding Lead (DSL). The Head of ICTis also a CEOP trained Ambassador and works collaboratively with the Assistant Headteacher, Pastoral to coordinate online safety strategy,
- Online safety training will be provided to staff as part of their wider annual safeguarding training and will include a focus on Child Sexual Exploitation (CSE) sexual harassment and violence and extremism and radicalisation.
- All staff will complete online safety training (National College) throughout the year to ensure that they are up to date with important developments. Pastoral leaders will complete enhanced online safety training annually.
- All staff will participate in the Workshop Raising Awareness of Prevent (WRAP) to ensure that they are aware of how the Internet and Social Media is used to radicalise individuals.
- A 'Safeguarding Bulletin' is issued to all staff at least once every term and includes regular guidance and support for staff on responding to incidents of online safety.

- All staff are reminded of their responsibilities with respect to online safety through regular briefing updates, safeguarding foci of the week and regular reminders from key individuals within Holte.
- All staff undergo safeguarding and child protection training (including online safety) at induction.
- All new staff receive the school online safety, Safeguarding and Child Protection Policies and Keeping Children Safe in Education (September 2022) and the school ensure that these documents are understood.
- Online safety will be an important part of pastoral meetings held throughout the academic year. Specific training opportunities will be identified by the Deputy Headteacher – Inclusion.
- The Designated Safeguarding Lead and Assistant Headteacher - Pastoral will receive regular updates through the Local Authority and/or other information/training sessions and by reviewing guidance documents released.

7. Monitoring and responding to incidents of online safety

7.1 All use of the school's Internet access is logged and the logs are randomly but regularly monitored using Entrust. Entrust is used to enforce the school's AcceptableUse Policy for all computer use within the school and Virtual Learning Environment (VLE). Entrust provides fast and accurate management data that allows the school to deal swiftly and effectively with any instances of misuse that occur. The outcome data is recorded and used to heighten awareness of the issues highlighted and will support all usersin the development of increased online safety skills. This data is shared with and reviewed by the school's governing body.

7.2 Any breaches, suspected or actual, of the school's Acceptable Use Policy are reported immediately to the Headteacher and Designated Safeguarding Lead (DSL) through Entrust. All 'captures' are graded according to severity and are sent to the Headteacher, DSL and DDSL via. email for their immediate attention. All incidents are logged using CPOMS.

7.3 Any member of staff employed by the school who comes across an online safety issue does not investigate any further but immediately reports it to the Deputy Headteacher – Inclusion or Assistant Headteacher - Pastoral and impounds the equipment. If the concern involves a member of staff then the member of staff should report the issue to the Headteacher.

7.4 The school recognises that there is a risk that filtering and monitoring systems may be bypassed by students or adults. Any online safety incidents must therefore immediately be reported to the Headteacher (if a member of staff) or Deputy Headteacher – Inclusion/Assistant Headteacher-Pastoral (if a student) who will investigate further following online safety and safeguarding policies and guidance. Whenever any inappropriate use is detected it will be followed up by either Year Managers, Year Coordinators, Assistant Headteacher - Pastoral or another member of SLT depending on the severity of the incident.

7.5 It is hoped that all members of the school community will be responsible users of ICT, who understand and follow this policy. However, there may be times when infringements of the policy could take place through careless or irresponsible, or very rarely, through deliberate misuse. If any apparent or actual misuse appears to involve illegal activity e.g. child sexual abuse images, adult material which potentially breaches the Obscene Publications Act, criminally racist material or other criminal conduct, activity or materials the Police will be contacted in the case of a student while the LADO will be contacted in the case of a member of staff to discuss a suitable course of action. If members of staff suspect that misuse might have taken place, but that the misuse is not illegal (as above) it isessential that correct procedures are used to investigate, preserve evidence and protect those carrying out the investigation. It is recommended that more than one member of staff

is involved in the investigation which should be carried out on a “clean” designated computer. It is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the school community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal behaviour/disciplinary procedures.

8. Cyberbullying

8.1 The rapid development of, and widespread access to, technology has provided a new medium for 'virtual' bullying, which can occur in or outside school. Cyber-bullying is a different form of bullying and can happen at all times of the day, with a potentially bigger audience, and more accessories as people forward on content at a click.

8.2 The Education Act 2011 amended the power in the Education Act 1996 to provide that when an electronic device, such as a mobile phone, has been seized by a member of staff who has been formally authorised by the headteacher, that staff member can examine data or files, and delete these, where there is good reason to do so. This power applies to all schools and there is no need to have parental consent to search through a young person's mobile phone.

8.3 If an electronic device that is prohibited by the school rules has been seized and the member of staff has reasonable ground to suspect that it contains evidence in relation to an offence, they must give the device to the police as soon as it is reasonably practicable. Material on the device that is suspected to be evidence relevant to an offence, or that is a pornographic image of a child or an extreme pornographic image, should not be deleted prior to giving the device to the police. If a staff member finds material that they do not suspect contains evidence in relation to an offence, they can decide whether it is appropriate to delete or retain the material as evidence of a breach of school discipline.

8.4 Cyber-bullying (along with all other forms of bullying) of any member of the school community will not be tolerated. Full details are set out in the school's Behaviour Policy.

- There are clear procedures in place to support anyone in the school community affected by cyber-bullying.
- All incidents of cyber-bullying reported to the school will be recorded.
- There will be clear procedures in place to investigate incidents or allegations of Cyber-bullying.
- Pupils, staff and parents will be advised to keep a record of the bullying as evidence.
- The school will take steps to identify the bully, where possible and appropriate. This may include examining school system logs, identifying and interviewing possible witnesses, and contacting the service provider and the police, if necessary.
- Pupils, staff and parents will be required to work with the school to support the approach to cyber-bullying and the school's online safety ethos.
- Sanctions for those involved in cyber-bullying may include:
- The bully will be asked to remove any material deemed to be inappropriate or offensive.

- A service provider will be contacted to remove content if the bully refuses or is unable to delete content, including the following - https://swgfl.org.uk/services/report-harmful-content/report-harmful-content-button/
- Internet access may be suspended at school for the user for a period of time. Other sanctions for pupils and staff may also be used in accordance with the Whole School Behaviour Policy, Acceptable Use Agreement and Disciplinary Procedures.
- Parents of pupils will be informed. The Police will be contacted if a criminal offence is suspected.

9. Online safety in specific contexts

9.1 Extremism and radicalisation

The statutory guidance makes clear the need for schools to ensure that children are safe from terrorist and extremist material when accessing the internet in schools. Schools should ensure that suitable filtering is in place and students are safe from radicalisation whilst online.

More generally, schools have an important role to play in equipping children and young people to stay safe online, both in school and outside. Internet safety will usually be integral to a school's ICT curriculum and can also be embedded in Citizenship. Personal Social and Health Education and Relationships, Sex and Health Education.

As with other online risks of harm, every teacher needs to be aware of the risks posed by the online activity of extremist and terrorist groups and will receive annual training through in-school Safeguarding Training and the Workshop Raising Awareness of Prevent.

9.2 Peer on peer abuse

Online sexual harassment may be standalone, or part of a wider pattern of sexual harassment and/or sexual violence. This may include:

- Non-consensual haring of sexual images and videos.
- Sexualised online bullying.
- Unwanted sexual comments and messages, including on social media.
- Sexual exploitation, coercion or threats.

When an incident involves nude or semi-nude images and/or videos, the member of staff should refer the incident to the designated safeguarding lead (or deputy) as the most appropriate person to advise on the school's response.

9.3 Child on child sexual violence and sexual harassment

Sexual violence and sexual harassment can take place both online and offline. Further advice is available in the DfE guidance "Sexual violence and sexual harassment between children in schools and colleges".

In addition to fulfilling its legal responsibilities with respect to sexual violence and sexual harassment the school ensures that there is a whole school approach to preventing child on child sexual violence and harassment. All staff are aware of the processes and procedures for reporting such incidents, including for staff not to view or forward indecent images.

The DSL is aware of procedures for seeking the removal of indecent images, including referrals to the Internet Watch Foundation.

9.4 Child Sexual Exploitation

Child sexual exploitation (CSE) may involve the role of the internet to identify potential victims or as a tool to coerce and blackmail children into performing sexual acts, both on and offline. The internet may also be provided to children as a “gift” by perpetrators, for example in the form of new mobile phones and devices. CSE can also take place completely online, for example children being coerced into performing sexual acts via webcam; it may not always result in a physical meeting between children and the offender

9.5 Gang activity and County Lines

The internet can play a significant role in gang activity, such as gifts of technology and communication and intimidation over social media.

6. Parents, carers and Online Safety

10.1 Parent and carer's attention will be drawn to the school's online safety policy and on the school web site. The School will maintain a list of online safety resources for parents/carer's and share these as appropriate. Links to further safety information will be shared on the school's website.

10.2 Sites of use for parents, carer's, staff members and young people can be found below:

- https://www.saferinternet.org.uk/
- http://www.ceop.police.uk
- http://www.thinkuknow.co.uk
- https://www.nspcc.org.uk
- http://www.childnet.com
- http://parentzone.org.uk/

The school will organise parent workshops on online safety throughout the academic year and distribute information leaflets during school events such as parents' evenings.

Appendix One

Online technologies

Current and emerging technologies used in school and, more importantly in many cases, used outside of school by children include:

Internet	**Our School Approach**
The web	filtered by our own web filtering (Futures Cdoud), site blacklist
E-mail	Staff monitored accounts.
Instant messaging (e.g. MSN)	all blocked except use as part of delivering the curriculum
Blogs	moderated by teachers
Podcasting (radio / audio broadcasts downloaded to computer or MP3/4 player)	uploaded by HML ICT Network Manager
Social networking sites such as MySpace, Bebo, Piczo, Facebook	all blocked in school.
Video broadcasting sites such as YouTube	all blocked in school except allowed by staff for specific purpose.
Chat Rooms	all blocked in school.
Gaming Sites	blocked in school wherever possible except allowed by staff or needed for learning purposes. Use monitored using ABtutor.
Music download sites	blocked in school.
Wikis	moderated by teacher/HML ICT Network Manager
Non-Internet	**Our School Approach**
Mobile phones with camera and video functionality	all banned in school.
Mobile technology (e.g. games consoles) that are 'internet ready'.	banned, unusable in school.
Smart phones with e-mail, web functionality.	banned in school.

Appendix Two

Online safety agreement

Parents

- There are a number of important steps you can take to ensure your children are safer when using sites such as Facebook, Twitter, Instagram, Bebo, Snapchat, WhatsApp or KiK.
- Become familiar with the sites yourself
- Encourage your children to keep their profiles private.
- Be careful about what information your children are sharing on the sites. Do you know all of your child's online friends ?
- Encourage children to think about who they want to add as a friend.
- Make sure your children know where to go for help if they feel uncomfortable.
- If you don't want your children to access these services use parental control devices to block access to the sites.
- Remember that children must be 13 years or older to sign up for Facebook.
- Monitor the amount of time your child is spending on social networking sites.

Pupils

- Be careful with personal information. As soon as information goes online you have lost control over who will see it and how it will be used. Don't post pictures that you wouldn't want everyone to see.
- Don't assume everyone you meet online is who they appear to be. The information provided by users when they register is not checked. Anyone can create a profile pretending to be someone else.
- Don't post information that could be used to find you in the real world.
- Don't reply to messages that harass you or make you feel uncomfortable.
- Always explore the privacy settings of the site to protect your privacy and to protect yourself from strangers.
- Get your friends and family to check your social networking site to check you are doing things safely.
- Keep your passwords to yourself.
- If you are the victim of cyberbullying a) report the bully to the website b) keep evidence of what happened and c) tell an adult.
- Remember when you post something online you are posting it on the biggest screen in the world which can be seen by billions of people.
- Please sign below to show that you have read the above advice.

Signed

Pupil:_____

Parent:_____

Tutor:_____

Date:_____

Appendix Two

Advice for students and staff

Our advice for parents

- There are a number of important steps you can take to ensure your children are safer when using sites such as WhatsApp, KiK, Facebook, MySpace or Bebo.
- Become familiar with the sites yourself
- Encourage your children to keep their profiles private.
- Be careful about what information your children are sharing on the sites.
- Do you know all of your child's online friends ?
- Encourage children to think about who they want to add as a friend.
- Make sure your children know where to go for help if they feel uncomfortable.
- If you don't want your children to access these services use parental control devices to block access to the sites.
- Remember that children must be 13 years or older to sign up for Facebook.
- Monitor the amount of time your child is spending on social networking sites.
- Raise any concerns you have regarding your child immediately to your child's Year Co-ordinator.

Our advice for pupils

- Be careful with personal information. As soon as information goes online you have lost control over who will see it and how it will be used.
- Don't post pictures that you wouldn't want everyone to see.
- Don't assume everyone you meet on-line is who they appear to be. The information provided by users when they register is not checked. Anyone can create a profile pretending to be someone else.
- Don't post information that could be used to find you in the real world.
- Don't reply to messages that harass you or make you feel uncomfortable.
- Always explore the privacy settings of the site to protect your privacy and to protect yourself from strangers.
- Get your friends and family to check your social networking site to check you are doing things safely.
- Keep your passwords to yourself.
- If you are the victim of cyber-bullying a) report the bully to the website, b) keep evidence of what happened and c) tell an adult, d) report it using SHARP
- Remember when you post something on-line you are posting it on the biggest screen in the world which can be seen by billions of people.
- For more information on E-safety please visit, **www.thinkuknow.co.uk/parents**

Appendix Three

ICT Standards

Network

- Users may only use terminals they are personally logged on to.
- When logged on users must not allow others to use their terminal.
- Users must keep their password secret and secure.
- Users must change their password if they believe it is known by others.
- Users must use meaningful file names (i.e. not document 47).
- Users must log off when leaving their terminals.
- Users may only store school work on the network.
- Users must not attempt to override network security setting.

Documents

- All official school documents should have the official letter heading which includes the school logo.
- The number of fonts on a document should be limited to three.
- Important documents should be copied into a separate backup folder.

Printing

- No more than three copies should be printed on the network.
- User may only print work that they have developed or processed. This means you must not print pages directly from the internet.

Internet and Network Use

- Unauthorised use of a computer or network is against the law. (Computer Misuse Act 1990).
- Users are only authorised to use the network for school purposes.
- Users are not authorised to download files for personal use.

Internet safety

- Users must not give their or anybody else's personal details including names, addresses, phone numbers and photographs. This applies particularly in chat rooms and when sending emails.
- Users must not visit people unknown to them who they have met in chat rooms or forums.

Software

- User may not install software – copyright issue.
- Users may only use software installed by Authorised Network Staff.

Drinking, Eating and Seating

- Users who wish to drink water must move at least 1 metre from equipment.
- Eating is not allowed in the computer rooms at any time.
- Users must stand up and push wheeled chairs when moving them to another position in the room.

Appendix Four

Guidance for staff on responding to incidents of cyberbullying