Forty Hill CE Primary School
Online Safety Policy

Introduction

IT and Computing in the 21st Century is seen as an essential resource to support learning and teaching, as well as playing what is now regarded as an essential role in the everyday lives of children, young people and adults. Consequently, at Forty Hill CE Primary School, we need to ensure children are properly equipped with the skills to access IT and promote life-long learning and future economic well-being as members of the global community. Online safety involves pupils, staff, governors and parents making the best use of technology, information, training and this policy to create and maintain a safe online and ICT environment.

IT and Computing 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 IT within our society as a whole. Currently the internet technologies children and young people are using both inside and outside of the classroom include:

- Websites
- Learning Platforms and Virtual Learning Environments
- Email and Instant Messaging
- Chat Rooms and Social Networking
- Blogs and Wikis
- Podcasting
- Video Broadcasting
- Music Downloading
- Gaming
- Mobile/Smart phones with text, video and/or web functionality
- Other mobile devices with web functionality

Whilst exciting and beneficial both in and out of the context of education, much IT, 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. At Forty Hill, we understand the responsibility to educate our pupils in Online Safety issues; teaching them the appropriate behaviours and critical thinking to enable them to remain both safe and legal when using the internet and related technologies, in and beyond the context of the classroom.

This policy is inclusive of both fixed and mobile internet; technologies provided by the school; (such as PCs, laptops, iPads, webcams, whiteboards, digital video equipment, etc); and technologies owned by pupils and staff, but brought onto school premises (such as laptops, mobiles phones, camera phones and portable media players, etc).

Roles and Responsibilities

As Online Safety is an important aspect of strategic leadership within the school, the headteacher and governors have ultimate responsibility to ensure that the policy and practices are embedded and monitored. All staff share responsibility for online safety, however our Designated Safeguarding Leads and Deputy Designated Safeguarding Leads will act as our named Online Safety Leads. All members of the school community have been made aware of who holds these posts. It is the role of the Online Safety Leads to keep abreast of current issues and guidance through organisations such Enfield LA, LGFL, CEOP (Child Exploitation and Online Protection) and Childnet. The headteacher and Chair of Governors will ensure that all Governors have an understanding of the issues at our school in relation to local and national guidelines and advice in order that they remain updated.

Teaching and Learning

The Internet is an essential element for education, business and social interaction. Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils, and so Forty Hill CE Primary School has a duty to provide pupils with quality Internet access as part of their learning experience:

- The school Internet access will be designed expressly for pupil use including appropriate content filtering
- Pupils will be given clear objectives for Internet use and taught what use is acceptable and what is not through explicit Online Safety sessions, PSHE as well as during those lessons requiring the use of IT.
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation, including a development in the understanding that online content may be edited, filtered or designed to be persuasive.
- As part of the Computing curriculum, all year groups have digital literacy units that focus on different elements of staying safe online. These units include topics from how to use a search engine safely, ensuring our digital footprints are ones we are proud of and happy with and cyber bullying, including how to deal with this should it occur.
- The school will ensure that the use of Internet derived materials by staff and pupils complies with copyright law

Through ICT we ensure that the school meets the needs of all, taking account of gender, ethnicity, culture, religion, language, sexual orientation, age, ability, disability and social circumstances. It is important that in this school we meet the diverse needs of pupils to ensure inclusion for all and that all pupils are prepared for full participation in society. We also measure and assess the impact regularly through meetings with our SENCO and individual teachers to ensure all children have equal access and opportunities to succeed in this subject.

Pupils are taught in all lessons to be critically aware of the materials/content they access online and are guided to validate the accuracy of information. Pupils are taught to evaluate what they see, as well as consider the impact the content they are accessing has, or could have, on their mental wellbeing. Children will also be taught that images can be manipulated, including those that they have originally posted online themselves and how this can be used against them.

Authorised Internet Access

By explicitly authorising use of the school's Internet access, pupils, staff, governors and parents are provided with information relating to Online Safety and agree to its use:

- All staff must read and sign the 'Acceptable Use Policy' before using any school ICT resource
- Parents will be informed that pupils will be provided with supervised Internet access and asked to sign and return an Acceptable Use Policy to consent to its use
- Children will also be asked to read and sign an Acceptable Use Policy
- Only authorised equipment, software and Internet access can be used within the school

World Wide Web

The Internet opens up new opportunities and is becoming an essential part of the everyday world for children. However, there are inappropriate and undesirable elements that must be managed:

- If staff or pupils discover unsuitable sites, the URL (address), time, content must be reported to the school office and the Online Safety Lead or other senior member of staff, who will then contact the LGFL who provide our internet
- Pupils should be taught to be critically aware of the materials they are shown and how to validate information before accepting its accuracy
- Pupils should be taught to understand intellectual property rights

Email

E-mail is a quick and easy method of communication. Ensuring beneficial and appropriate usage is an important part of Online Safety:

- Pupils may only use approved e-mail accounts on the school system
- Pupils must immediately tell a teacher if they receive an offensive e-mail
- Pupils must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone (in person or in any virtual environment) without specific permission
- Access in school to external personal e-mail accounts may be blocked
- E-mail sent to external organisations should be written with professional standards with careful thought to how the school is represented and authorised before sending, in the same way as a letter written on school headed paper
- Chain letters, spam, advertising and all other emails from unknown sources will be deleted without opening or forwarding

Social Networking

Social networking Internet sites provide facilities to chat and exchange information online. This online world is very different from the real one with the temptation to say and do things beyond usual face-to-face contact:

- The school will block/filter access to social networking sites and newsgroups unless a specific use is approved
- Pupils will be advised never to give out personal details of any kind which may identify themselves, other pupils, their school or their location
- Pupils will be advised not to place personal photos on any social network space in their termly safety lessons
- Pupils and parents will be advised that the use of social network spaces outside school is inappropriate for primary aged pupils
- Pupils will be advised on security and encouraged to set passwords, deny access to unknown individuals and instructed how to block unwanted communications
- Pupils should be encouraged to invite known friends only and deny access to others
- Parents, pupils and staff will be advised of the dangers of discussing pupils, staff or the school on social networking sites. The Governors will consider taking legal action, where appropriate, to protect pupils, staff and the reputation of the school itself against cyber bullying and defamatory comments
- Parents will be regularly reminded not to publish images from school on social media platforms

Sexting

- Incidences involving sexting, the sharing of inappropriate sexual images, should refer to UKCISS "Sexting in Schools and Colleges" document and a meeting should be held by the DSL.
- The DSL will follow the Safeguarding policy to decide on the appropriate course of action and assess the risk posed to the child or children involved and whether this involves or requires a referral being made to the police and/or children's social care.

Mobile Phones

Many mobile phones have access to the Internet and picture and video messaging. Whilst these are the more advanced features, they present opportunities for unrestricted access to the Internet and sharing of images. There are risks of mobile bullying, or inappropriate contact.

- Pupils by permission of the headteacher can bring mobile phones onto the school site where it is seen by the school and parents as a safety/precautionary use. These are to be handed into the school office at 8.55am and collected at the end of the day
- The sending of abusive or inappropriate text messages is forbidden
- Staff should always use the school phone to contact parents and never their personal mobile
- Staff, parents, pupils and visitors are not permitted to access or use their mobile phones within the classroom
- Mobile phones should not be used by children, parents or staff in the school playground before, during or after school

- Mobile phones should not be used to make recordings or photos of any kind, nor for sharing of video or pictures that could include images of children other than their own
- Staff may use their mobile phones in the staffroom
- On trips, staff and parent mobile phones should be used for emergencies only

Digital/Video Cameras/Photographs/iPads

Pictures, videos and sound are not directly connected to the Internet but images are easily transferred.

- Pupils will not use digital cameras, iPads or video equipment at school unless specifically authorised by staff
- Publishing of images, video and sound will follow the policy set out in this document under 'Published Content'
- Parents and carers are permitted to take photos/videos of their own children in school events but are requested not to share these photos/videos on social networking sites if other pupils appear in the background
- The headteacher or a nominee will inform parent(s)/guardian(s) and others present at school events that photographs/videos may be taken on the basis that they are for private retention and not for publication in any manner
- Staff should always use a school camera to capture images and should not use their personal devices
- Photos taken by the school are subject to the Data Protection Act

Published Content and the School Website

The school website is a valuable source of information for parents and potential parents.

- Contact details on the website will be the school address, e-mail and telephone number.
- Staff and pupils' personal information will not be published
- The headteacher or a nominee will take overall editorial responsibility and ensure that content is accurate and appropriate
- Pupils' full names will not be used in association with photographs
- Consent from parents is obtained via the Home School Agreement so that pupils' photos can be published on the school website
- Work will only be published with the permission of the pupil
- Parents should only upload pictures of their own child/children onto social networking sites
- The Governing body may ban the use of photographic equipment by any parent who does not follow the school policy

Information System Security

- School ICT systems capacity and security will be reviewed regularly
- The school will take all reasonable steps to ensure protection against virus and cyber-attack, installing and updating virus protection regularly
- Security strategies will be discussed with LGFL

Protecting Personal Data

Personal data will be recorded, processed, transferred and made available according to GDPR regulations and guidance from the Local Authority Data Protection Officer.

Assessing Risk

- The school will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked Internet content, it is not possible to guarantee that unsuitable

material will never appear on a school computer. The school or Local Authority does not accept liability for the material accessed, or any consequences of Internet access
- The school will audit ICT use to establish if the Online Safety policy is adequate and that the implementation of the Online Safety policy is appropriate

Reporting Breaches of Online Safety

- All breaches of the Online Safety policy need to be recorded on ScholarPack via the Online Safety tab. The details of the user, date and incident should be reported
- Incidents which may lead to child protection issues will be dealth with by the school through the child protection and safeguarding procedures, being passed on to one of the Designated Teachers immediately – it is their responsibility to decide on appropriate action, not the class teachers
- Incidents which are not child protection issues but may require headteacher intervention (e.g. cyberbullying) should be reported to the headteacher on the same day
- Allegations involving staff should be reported directly to the headteacher or, if concerning the headteacher, directly to the Chair of Governors
- Evidence of incidents must be preserved and retained
- The curriculum will cover how pupils should report incidents (e.g. CEOP button, trusted adult, Childline)

Handling Online Safety Complaints

- Complaints of Internet misuse will be dealt with by a senior member of staff
- Any complaint about staff misuse must be referred to the headteacher
- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures
- Parents wishing to complain about Online Safety issues should use the established school complaints procedure
- Discussions will be held with the Community Police to establish procedures for handling potentially illegal issues

Communication of the Online Safety Policy

Pupils:

- Rules for Internet access and Online Safety will be posted in the computer suite
- Pupils will be informed that Internet use will be monitored
- Pupils will be informed of the importance of being safe on social networking sites. This will be strongly reinforced across all year groups during computing/ICT lessons

Staff:

- All staff will be informed about, and given access to, the school Online Safety policy and its importance explained
- Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential

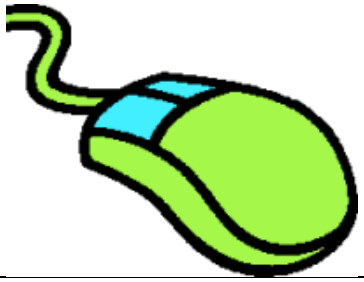
Parents:

- Parents' attention will be drawn to the school Online Safety policy in newsletters, the school prospectus and on the school website

Accepted by the Governing Body: February 2020
Review Date: February 2023

Forty Hill CE Primary School
Acceptable Use of Technology Agreement: KS1 Children

Think before you click!



S 	**I will only use the Internet and email with an adult present**
A 	**I will only click on icons and links when I know they are safe**
F 	**I will only send friendly and polite messages to people I know in real life and only if an adult says it is ok to**
E 	**If I see something I don't like on a screen, I will always tell an adult**

With the help of my teacher I have read and understand these rules. I will try my best to follow them.

Name: ***Date:***





Forty Hill CE Primary School
Acceptable Use of Technology Agreement: KS2 Children

For my own personal safety:

- I will not take part in online challenges
- I will treat my username and password like my toothbrush – I will not share it, nor will I try to use any other person's username and password.
- I am aware that some websites, social networks, games and APPs have age restrictions and I should respect this.
- I will only e-mail people I know, or a responsible adult has approved.
- I will be aware of "stranger danger", when I am communicating on-line.
- I will not give my home address, phone number, send a photograph or video, or give any other personal information, including my school name, that could be used to identify me, my family or my friends, unless a trusted adult has given permission.
- I will never arrange to meet someone I have only ever previously met on the Internet or through a game, unless my parent/carer has given me permission and I take a responsible adult with me.
- I will immediately report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it on-line and I will not live stream content.
- I know that not everything I see online is real and that some content is filtered or edited and I will think about why someone would do this.
- If content ever makes me feel sad or upset about myself, or I worry that I spend too much of my time online, I will speak to a trusted adult.
- If my parents feel that I need to bring my mobile phone to school, I will hand it in to the office each morning.

I will act as I expect others to act towards me:

- I will only send or upload polite and sensible messages or images on the computer or my phone.
- I understand that nasty/hurtful messages would be considered as cyberbullying.
- I will not take or distribute images of anyone without their permission.
- I will only edit or delete my own files and not look at, or change, other people's files without their permission.

When using the internet for research:

- I will only use other people's writing, pictures, music or video if I know I have legal copyright permission.

Keeping our school system secure:

- I understand that the school will monitor my use of the ICT systems, email and other digital communications.
- I will not open an attachment, or download a file, unless I know and trust the person who has sent it.
- I will not attempt to visit Internet sites that I know to be banned by the school.
- I will only use the school's computers for schoolwork and homework.
- I will not bring files into school without permission or upload inappropriate material to my workspace.

I have read and understand these rules and agree to them.

Name: ***Date:***





Forty Hill CE Primary School
Acceptable Use of Technology Agreement: Parents

Internet and ICT:
As the parent or legal guardian of the pupil named below, I grant permission for the school to give my child access to:

- the Internet at school
- the school's education email system
- the school's online Managed Learning Environment (MLE)
- ICT facilities and equipment at the school.

- I know that my child has signed an Acceptable Use Agreement and will receive regular Online Safety education to help them understand the importance of safe use of ICT – both in and out of school.
- I accept that ultimately the school cannot be held responsible for the nature and content of materials accessed through the Internet and mobile technologies, but I understand that the school takes every reasonable precaution, including monitoring and a web filtering system to keep pupils safe and to prevent pupils from accessing inappropriate materials.
- I understand that the school can, if necessary, check my child's computer files and the Internet sites they visit at school and if there are concerns about my child's e-safety or e-behaviour they will contact me.

Use of digital images, photography and video:

- I understand that the school's Online Safety Policy covers the use of digital images and video and I support this.
- I understand that the school may use photographs of my child or include them in video material to support learning activities.
- I accept that the school may use photographs / videos that include my child in publicity that reasonably promotes the work of the school, and for no other purpose.
- I will not take and then share online, photographs of other children (or staff) at school events without permission.

Social networking and media sites:

- I understand that the school's Online Safety Policy covers the use of social networking and media sites and I support this.
- I understand that the school takes any inappropriate behaviour seriously and will respond to observed or reported inappropriate or unsafe behaviour.
- I will support the school by promoting safe use of the Internet and digital technology at home. I will inform the school if I have any concerns.

My child's name:

Parent / guardian signature: **Date:**





Forty Hill C of E Primary School:
Acceptable Use of Technology Agreement: Staff

I understand that I must use school ICT systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the ICT systems and other users. I recognise the value of the use of ICT for enhancing learning and will ensure that pupils receive opportunities to gain from the use of ICT. I will, where possible, educate the young people in my care in the safe use of ICT and embed e-safety in my work with young people.

For my professional and personal safety:

- I understand that the school may monitor my use of the ICT systems, email and other digital communications.
- I understand that the rules set out in this agreement also apply to use of school ICT systems (eg laptops, email, MLE etc) out of school.
- I understand that the school ICT systems are primarily intended for educational use and that I will not use the systems for inappropriate personal or recreational use.
- I will not disclose my username(s) or password(s) to anyone else, nor will I try to use any other person's username and password. I will follow 'good practice' advice in the creation and use of my password. If my password is compromised, I will ensure I change it.
- I will not allow unauthorised individuals to access email / Internet / intranet / network, or other school systems
- I will immediately report any illegal, inappropriate or harmful material/incident I become aware of, to the appropriate person.

I will be professional in my communications and actions when using school ICT systems:

- I will not access, copy, remove or otherwise alter any other user's files, without their express permission.
- I will communicate with others in a professional manner; I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will only use the approved, secure LGfL email system(s) for any school business.
- I will ensure that when I take and / or publish images of others I will do so with their permission and in accordance with the school's policy on the use of digital / video images. I will not use my personal equipment to record these images. Where these images are published on the school website it will not be possible to identify by name, or other personal information, those who are featured.
- I will ensure that digital imagery/video posted on the MLE will be restricted to children whose parents have given permission.
- I will not use chat or social networking sites on school equipment or during the school day.
- I will only communicate with pupils and parents / carers using official school systems. Any such communication will be professional in tone and manner.
- I will not use my personal mobile phone to communicate with parents unless permission has been given by the Headteacher in exceptional circumstances.
- I will not use personal digital cameras or camera phones for taking and transferring images of pupils or staff and will not store images at home
- I will not engage in any on-line activity that may compromise my professional responsibilities and will adhere to the school code of conduct at all times on social media.
- I will ensure that any private social networking sites / blogs etc that I create or actively contribute to do not contradict the Code of Conduct.
- I will not 'friend' pupils or parents on my private social networking site and will ensure my privacy settings prevent wider public accessing my personal profile.

The school is responsible for providing safe and secure access to technologies and ensure the smooth running of the school:

- I will embed the school's Online Safety curriculum into my teaching.
- I will access school resources remotely through the MLE and will ensure any pupil data is not seen by others and not stored on a home computer.

- I understand that my personal mobile phone / device must be switched off and out of sight during teaching time, unless express permission has been given by the Headteacher in exceptional circumstances. I will not wear earphones in class or around the school.
- I will not open any attachments to emails, unless the source is known and trusted, due to the risk of the attachment containing viruses or other harmful programmes.
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.
- I understand that the data protection policy requires that any staff or student / pupil data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by school policy to disclose such information to an appropriate authority.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.

When using the internet in my professional capacity or for school sanctioned personal use:

- I will ensure that I have permission to use the original work of others in my own work
- Where work is protected by copyright, I will not download or distribute copies (including music and videos).

I understand that I am responsible for my actions in and out of school:

- I understand that this Acceptable Use of Technology Agreement applies not only to my work and use of school ICT equipment in school, but also applies to my use of school ICT systems and equipment out of school and my use of personal equipment in school or in situations related to my employment by the school.
- I understand that if I fail to comply with this Acceptable Use of Technology Agreement, I could be subject to disciplinary action. This could include a warning, a suspension, referral to Governors and / or the Local Authority and in the event of illegal activities the involvement of the police.
- I understand that it is my duty to support a whole-school safeguarding approach and will report any behaviour (of other staff or pupils), which I believe may be inappropriate or concerning in any way, to the designated child protection officer at the school

I have read and understand the above and agree to use the school ICT systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) within these guidelines.

Staff Name:

Signed: **Date:**