SOMERVILLE FEDERATION

Promoting Digital Safety Policy

March 2022

Contents

Our Digital Safety Policy

The school's digital safety Coordinator is the head teacher; Mr Phil Dickson. This policy is reviewed by the safeguarding team led by our Designated Safeguarding Lead (Mr Phil Dickson) and our computing team is led by Mrs Kirstie Sloan.

School website will be constantly updated with useful links related to this policy:

Introduction to Digital Safety

1.1 Digital Safety in a Changing World

At Somerville Primary School, we celebrate the value and importance of technology in our children's learning. In our school; personal computers, wireless laptops, I-pads, digital voice recorders, camcorders and digital cameras are all part of children's every day learning. The internet has become a vital source of learning and communication for all members of our school community.

Pupils interact with new technologies such as mobile phones and the Internet on a daily basis and experience a wide range of opportunities, attitudes and situations. The exchange of ideas, social interaction and learning opportunities involved are greatly beneficial but can occasionally place young people in danger.

Our school seeks to provide the right balance between controlling access, setting rules and educating students for responsible use.

We currently have nearly 100 iPads, 60 tablets, 60 laptops and 120 Chromebooks alongside the 20 desktop Computer suite.

The term digital safety covers the issues relating to how our school ensures that young people are safe and guided in their use of the Internet; apps; mobile phones and other electronic communication technologies. This policy assesses the protocols for ensuring that these initiatives are carefully developed in our school, so that we progress responsibly and appropriately in the interests of our children. It also looks at how we educate our children to be safe in a world where technology is so readily available. Policy is also concerned with the safety controls in place for staff.

Protecting young people and adults properly means thinking beyond the school environment. Broadband, Wi-Fi and 3/4G connections now mean the world wide web is available anywhere, anytime. Moreover, the introduction of the internet on games consoles, tablets and mobile phones mean it is becoming increasingly difficult to safeguard our children from the dangers hidden in cyberspace. Our children will not only be working online in school or at home; their personal devices are not always covered by network protection and it is, therefore, imperative that they are educated on the risks involved with using the internet, apps and other digital communication so they provided with guidance and a range of strategies on how to act if they see, hear or read something that makes them feel uncomfortable.

Effective Practice in Digital Safety

digital safety depends on effective practice in each of the following areas:

- Education for responsible ICT and computing use by staff and pupils. We require clear expectations of behaviour and/or codes of practice relevant to responsible use of the internet for educational, personal or recreational use.
- A comprehensive, agreed and implemented digital safety Policy;
- Secure, filtered broadband that the school manages with our partners the Local Authority ITSOS teams Internet filter (SimplICT);
- Effective school based training. digital safety is reviewed annually as part of our safeguarding training. We also have a number of staff who are level 2 trained in online exploitation and cyber bullying used our accredited and assessed Edu Care and National College online training.
- Policy and systems that assists school staff working with children to work safely and responsibly with the internet and other communication technologies and to monitor their own standards and practice.
- Clear structures to deal with online abuse, such as online bullying, which are cross referenced with other school policies.
- Ensure that all members of the school community are aware that unlawful or unsafe behaviour is unacceptable and that, where appropriate, disciplinary or legal action will be taken.

1.2 Digital Safety and the Legal Issues

Digital safety should be practiced to protect children, staff and all members of our school community. Our School's digital safety Policy is designed to raise awareness and address safety issues associated with information systems and electronic communications as a whole.

Our digital safety commitments are fully linked to our safeguarding policy, anti-bullying policy and the school's Prevent Duty.

Digital safety encompasses not only Internet technologies and apps but also electronic communications such as mobile phones and wireless technology. It highlights the need to educate children and young people about the benefits, risks and responsibilities of using information technology. It provides safeguards and raises awareness to enable users to control their online experiences.

The Internet is an unmanaged, open communications channel. The World Wide Web, e-mail, blogs and social networking all transmit information using the Internet's communication infrastructure internationally at low cost. Anyone can send messages, discuss ideas and publish material with little restriction. These features of the Internet make it an invaluable resource used by millions of people every day.

Much of the material on the Internet is published for an adult audience and some is unsuitable for pupils. In addition, there is information on weapons, crime and racism access to which would be more restricted elsewhere. Pupils must also learn that publishing personal information could compromise their security and that of others.

Schools need to protect themselves from legal challenge. The law is catching up with Internet developments: for example, it is a criminal offence to store images showing child abuse and to use e-mail, text or Instant Messaging (IM) to 'groom' children. In addition, there are many grey areas for schools to consider regarding communication of social network sites, storage of data etc.

Schools can help protect themselves by making it clear to pupils, staff and visitors that the use of school equipment for inappropriate reasons is "unauthorised". However, schools should be aware that a disclaimer is not sufficient to protect a school from a claim of personal injury and the school needs to ensure that all reasonable actions have been taken and measures put in place to protect users.

In practice this means that this school ensures that;

- It has effective firewalls and filters on our school network.
- Ensures that digital safety responsibilities are clearly communicated to all members of our school community.
- That our Acceptable Use Policies are fully enforced for children, staff and visitors. This includes supply teachers, volunteers and associate teachers.
- Ensures that our procedures are consistent with the Data Protection Act and GDPR regulations.

Learning and Teaching in the Digital Age

The school uses wireless laptops, mobile devices and comprehensive broadband access to develop learning and teaching through digital communication. Access to instant messenger services and mobile phones is not allowed as part of this school's curriculum. However, the school will include provision to educate children how to use this technology appropriately and safely.

2.1 Why the Internet and digital communications are important

Mobile digital devices and the Internet are an essential element in 21st century life for education, business and # social interaction. The school has a duty to provide pupils with quality Internet access as part of their learning experience. We also recognise that children are actively engaged with digital communication form an early age. It is part of their lifelong learning experiences and habits. This generation are what Marc Prensky refers to as 'digital natives'. We have to embrace that opportunity. However, we also have a responsibility to ensure that our children learn to use these opportunities and resources responsibly, appropriately and productively to enhance their learning

In addition, use of the Internet is a part of the statutory curriculum and a necessary tool for staff and pupils.

2.2 Encouraging responsible use of the Internet and digital communication.

1. The school Internet access is designed expressly for pupil use and includes filtering appropriate to the age of pupils. This is arranged through the school's needs with our partners at the Local Authority internet filtering and the school's network arrangements. Only sites directly approved by either the executive head teacher or the school's business manager will be allowed to override the filter. Details about our internet filtering can be found at:

   https://surfprotect.co.uk/

   We have chosen this because of the high quality internet filtering.

   The IWF publishes a list of websites which contain indecent images, advertisements for, or links to such content. This list is automatically incorporated behind the scenes into SurfProtect Quantum twice daily to ensure that these websites are instantly blocked to users

2. Pupils will be taught about responsible and appropriate information sharing through the internet and other forms of digital communication and apps.
3. Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.
4. Pupils will be taught about responsible use of e-mails and other sources of digital communication including e-mail, messenger services and texts.
5. Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation
6. Pupils will be shown how to publish and present information to a wider audience safely and responsibly.

2.3 Pupils will be taught how to evaluate Internet and other digital communication content

- The school will ensure that the use of Internet derived materials by staff and pupils complies with copyright law.
- Pupils will be taught the importance of cross-checking information before accepting its accuracy.
- Pupils will be taught how to report unpleasant Internet or other digital content including messages, e-mails and texts. Whilst we cannot promote the use of social networking sites, we must also ensure that our children know how to manage the risks and dangers associated with these activities.

Managing Digital Access, Communication and Content

All Internet accessed is managed by the school. Individual users should only access the Internet through their username and password. The school recognises that password protection is a vital element of promoting digital safety.

Pupils cannot use mobile phones or other personal devices in school.

Staff or visitors cannot put unauthorised devices on network. Authorised use guidance states that they cannot access inappropriate content on mobile (non-school) networks.

The school will ensure that permission for access to internet and use of any content including photographs is fully explained and sought.

3.1 Information system security

- School's digital systems security will be reviewed regularly. This will be part of the liaison between the executive head teacher and our partners at the Local Authority.
- Virus protection and internet filtering will be updated regularly as part of the school's Service Level Agreement with the LA.
- Security strategies will be discussed with the LA.
- Remote access will be password protected.
- Passwords will automatically be renewed monthly.

3.2 Managing filtering

The school will work with the Local Authority to ensure systems work effectively:

- If staff or pupils come across unsuitable on-line materials, the site must be reported to the digital safety Coordinator (the head teacher).
- Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable. This will include searching for content related to inappropriate images, radicalisation and non-education content. Our Guidance on internet filtering has been updated following the introduction of the Prevent Duty in 2015.
- We use a software package called fusion that allows us to track and monitor all internet use.
- When the executive head teacher checks internet filters he will e-mail DHT and the Local Authority to warn them the system is being tested.
- Our technician also ensures that our filtering and blocking is regularly updated.

3.3 E-mail

- Pupils may only use their school approved gmail account on the school system from April 2021). All use of other e-mail accounts are prohibited. This is a completely internal mail system locked down to their class. All mail is screened with inappropriate use reports immediately sent to the class teacher.
- Staff should only use school approved e-mail accounts at work. We have a g-mail .somerville.wirral.sch.uk, clear guidance for what constitutes professional use of e-mail is included in the Acceptable Use agreements. However, we are absolutely clear that staff cannot use e-mail to communicate personal opinions that may be defamatory or abusive to individuals or organizations associated with the school.
- Pupils must immediately tell a teacher if they receive offensive e-mail/message.

- In e-mail communication, pupils must not reveal their personal details or those of others, or arrange to meet anyone without specific permission.
- Incoming e-mail should be treated as suspicious and attachments not opened unless the author is known. If in doubt staff will seek advice from Hi-Impact technicians.
- The school does not allow direct contact through personal e-mail for any professional correspondence. Any communication with other organizations, schools etc must be controlled through the authorised e-mail account.

3.4 Published content and the school web site

- Staff or pupil personal contact information will not generally be published. The contact details given online are the school office.
- The executive head-teacher will take overall editorial responsibility and ensure that content is accurate and appropriate. Governing Body understands their statutory duties in respect of information that should be available on the school website.

3.5 Publishing pupil's images and work

- Photographs that include pupils will be selected carefully so that individual pupils cannot be identified or their image misused. Consider using group photographs rather than full-face photos of individual children. The school will always risk assess photographs for possible abuse.
- Names or any other personal details will not normally published alongside photographs. If the photographs celebrate an award etc. permission will be sought to use photograph and name.
- Pupils' full names will not be used on a school Web site or other on-line space, in association with photographs.
- Work can only be published with the permission of the pupil.
- Pupil image file names will not refer to the pupil by name.
- Parents should be clearly informed of the school policy on image taking and publishing. We have an explicit permission slip for this.

3.6 Social networking and personal publishing

- The school will control access to social networking sites, and consider how to educate pupils in their safe use.
- Pupils will be advised never to give out personal details of any kind which may identify them, their friends or their location.
- Pupils and parents will be advised that the use of social network spaces outside school brings a range of dangers for primary aged pupils.
- Pupils will be advised to use nicknames and avatars when using the Virtual Learning Environment.
- Staff are fully informed of their responsibilities regarding the use of social networking sites such as Facebook, Twitter, Instagram etc. At Somerville Primary we have agreed that we should separate professional and personal commitments on these sites. Therefore, the following groups cannot be allowed as contacts and friends;
    - Ex pupils. Many of these sites are targeted at adults. It is not appropriate to have contacts in this context who are under 18. In addition, the context of teacher to pupil relationship is not suitable for social networking.
    - Parents. We believe that it is unfair on parents and staff to complicate the professional relationship that exists within school through the use of social networking sites. It is both inappropriate and open to abuse.

- All staff are aware that they could face charges of gross misconduct if they use social networking platforms to communicate personal opinions that may be defamatory or abusive to individuals or organizations associated with the school. This is not private correspondence.

3.7 Managing videoconferencing & webcam use

- Videoconferencing should use the educational broadband network to ensure quality of service and security.
- Video conferencing for pupils can only take place under the direct supervision of a member of staff.
- Staff engaging in video conferencing are advised that the normal standards of professional behavior apply.

3.8 Managing mobile technologies

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed. Currently mobile phones are not to be used in school by pupils. Staff and children have explicit guidance on mobile phones (see mobile phone policy).
- The executive team should note that technologies such as mobile phones with wireless Internet access can bypass school filtering systems and present a new route to undesirable material and communications. **This is addressed in our mobile phones at School policy.**
- Mobile phones will not be used during lessons or formal school time. The sending of abusive or inappropriate text messages or files by Bluetooth or any other means is forbidden.
- The use by pupils of cameras in mobile phones is not allowed in school or on trips etc.
- Staff are not allowed to use mobile phones to take or store images.
- Games machines including the Sony Playstation, Microsoft Xbox and others have Internet access which may not include filtering. Care is required in any use in school or other officially sanctioned location.
- Staff will be issued with a school phone where contact with pupils is required or where mobile phones are used to capture photographs of pupils. Staff must not take photographs on their personal phones unless it is authorized by a senior member of staff. Staff have access to work cameras, I-pads etc.

3.9 Protecting and storing sensitive data

- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998. This information will be clearly communicated to all staff, including office staff on an annual basis.

Staff are aware that they have a professional responsibility to ensure the following;

- All laptops must be password protected. Work laptops cannot be used for the storage of any inappropriate material.
- All data and images of children must be carried on encrypted memory pens. These are issued to staff.
- Photographs cannot be stored on personal laptops or devices. The only exceptions are E-Profile data and the archive stored by the executive head teacher.
- All photographs must be stored on the school's secure Staff Drive on the administration network.
- No data or images can be transported out of the school without the device being approved or password protected. This includes digital cameras etc.
- Any personal devices must be password protected if staff bring them onto school premises (I-pads, mobile phones etc). These cannot be connected to the school network.

Developing Policy on digital safety

The pace of change with emerging technology means that all staff have to be vigilant about risks concerned with digital safety. School Policy has to be proactive and clear.

The responsibility for ensuring the effective implementation of digital safety policies is the head teacher's. Individual members of staff have responsibilities under their pay and conditions to ensure that these policies are followed. Clear advice is issued by professional organisations such as the NUE, NAHT, UNISON etc on these matters.

The Governing Body will consider these matters. Many duties will be devolved to the Health and Safety Committee. The Governing Body will exercise their duty to ask the head teacher to consider any matters arising from policy reviews.

4.1 Authorising Internet access

- All staff must read and sign the 'Staff Code of Conduct for ICT' before using any school ICT resource.
- The school will maintain a current record of all staff and pupils who are granted access to school ICT systems.
- At Key Stage 1, access to the Internet will be by adult demonstration with directly supervised access to specific, approved on-line materials.
- All Parents/Carers will be asked to sign and return a consent form.
- Includes governors, PTA, visitors, student teachers etc.

4.2 Assessing risks

- The school will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a computer connected to the school network. Neither the school nor the Local Authority can accept liability for any material accessed, or any consequences of Internet access.
- The school should audit ICT use to establish if the digital safety policy is adequate and that the implementation of the digital safety policy is appropriate and effective.
- We will assess all emerging and new technologies for their benefit and risk before they are introduced to the school.

4.3 Handling digital 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 head-teacher.
- Any complaints about the head teacher must be referred to the safeguarding officer. If they require investigation they must be referred to the chair of Governors.
- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.
- Pupils and parents will be informed of the complaints procedure.
- Pupils and parents will be informed of consequences for pupils misusing the Internet.
- Discussions will be held with the Police Youth Crime Officer to establish procedures for handling potentially illegal issues.

4.4 Community use of the network and Internet

- Through extended schools use and partnership with other organisations there may be wider community use of the school's network. The school will liaise with local organisations to establish a common approach to digital safety.
- All consent forms must be used for these groups.

Communicating the digital safety Policy

5.1 Introducing the digital safety policy to pupils

- **Digital Safety** rules will be posted in all rooms where computers are used and discussed with pupils regularly.
- Pupils will be informed that network and Internet use will be monitored and appropriately followed up.
- A programme of training in digital safety will be developed, possibly based on the materials from CEOP and Edu Care and National College accredited training on online exploitation and cyber bullying.
- Digital safety training will be embedded within the computing scheme of work and our Personal Social and Health Education (PSHE) curriculum.
- Our digital leaders will take in role in promoting this policy and wider digital safety issues.

5.2 Staff and the digital safety policy

- All staff will be given access to the School's digital safety Policy and its importance explained.
- digital safety will be a focal point for staff and volunteer induction. Staff must be informed that network and Internet traffic can be monitored and traced to the individual user.
- Staff that manage filtering systems or monitor ICT use will be supervised by senior management and work to clear procedures for reporting issues.
- Staff will always use a child friendly safe search engine when accessing the web with pupils. We use google with safe filtering enabled.

5.3 Enlisting parents' and carers' support

- Parents" and carers" attention will be drawn to the school's digital safety policy in newsletters and on the school Web site.
- The school will maintain a list of digital safety resources for parents/carers.

Appendix One: - Digital -Safety Curriculum

Pupil online safety curriculum

Teaching and learning

1.1. Our school has a clear, progressive online safety education programme as part of the computing/PSHE curriculum. This covers a range of skills and behaviours appropriate to the age of the children, including:

- To STOP and THINK before they CLICK.
- To develop a range of strategies to evaluate and verify information before accepting its accuracy.
- To know how to narrow down or refine a search.
- To understand acceptable behaviour when using an online environment/email, i.e. be polite, no bad or abusive language or other inappropriate behaviour; keeping personal information private.
- To understand why online 'friends' may not be who they say they are and to understand why they should be careful in online environments.
- To understand why they should not post or share detailed accounts of their personal lives, contact information, daily routines, location, photographs and videos and to know how to ensure they have turned-on privacy settings.
- To have strategies for dealing with receipt of inappropriate materials.
- To understand risks associated with contacting/communicating with individuals that ehy don't know.
- To understand the impact of online bullying, sexting, extremism and trolling and know how to seek help if they are affected by any form of online bullying.
- To know how to report any abuse, including online bullying, and how to seek help if they experience problems when using the internet and related technologies, i.e. parent, teacher or trusted staff member, or an organisation such as Childline or the CLICK CEOP button.

1.2. Teachers plan internet and apps use carefully to ensure that it is age-appropriate and supports the learning objectives for specific curriculum areas.

1.3. The school will remind pupils about their responsibilities through a Acceptable Use Agreement.

1.4. All staff will model safe and responsible behaviour in their own use of technology during lessons.

Online risks

1.5. Our school recognises that pupils increasingly use a range of technology such as mobile phones, tablets, games consoles and computers. It will support and enable children to use these technologies for entertainment and education but will also teach children (in PSHE) that some adults and young people will use such outlets to harm children.

Cyber bullying and abuse

1.6. Cyber bullying can be defined as "Any form of bullying which takes place online or through smartphones and tablets." - BullyingUK

1.7. Complaints of online bullying are dealt with in accordance with our Anti-Bullying Policy. Complaints related to child protection are dealt with in accordance with school/LA child protection procedures.

1.8. Through the PSHE curriculum, children are taught to tell a responsible adult if they receive inappropriate, abusive or harmful emails or text messages. We use worry boxes to support with this.

1.9. Posters providing information about how to get help from Childline, ThinkUKnow and the NSPCC are displayed in school and signposted online through the Federation Website.

1.10. Cyber bullying will be treated as seriously as any other form of bullying and will be managed through our anti-bullying and confiscation procedures. 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 policy on anti-bullying and behaviour.

1.11. There are clear procedures in place to support anyone in the school community affected by cyber bullying.

1.12. All incidents of cyber bullying reported to the school will be addressed by a senior member of staff.

Sexual exploitation/sexting

1.13. Sexting between pupils will be managed through our anti-bullying and confiscation procedures.
1.14. All staff are made aware of the indicators of sexual exploitation and all concerns are reported immediately to the DSL.
1.15. There are clear procedures in place to support anyone in the school community affected by sexting.
1.16. All incidents of sexting reported to the school will be recorded.

Radicalisation or extremism

1.17. Radicalisation refers to the process by which a person comes to support terrorism and forms of extremism leading to terrorism.
1.18. Extremism is defined by the Crown Prosecution Service as "The demonstration of unacceptable behaviour by using any means or medium to express views which:
- Encourage, justify or glorify terrorist violence in furtherance of beliefs.
- Seek to provoke others to terrorist acts.
- Encourage other serious criminal activity or seek to provoke others to serious criminal acts.
- Foster hatred which might lead to inter-community violence in the UK."

1.19. The school understands that here is no such thing as a "typical extremist": those who become involved in extremist actions come from a range of backgrounds and experiences, and most individuals, even those who hold radical views, do not become involved in violent extremist activity.
1.20. The school understands that pupils may become susceptible to radicalisation through a range of social, personal and environmental factors – it is known that violent extremists exploit vulnerabilities in individuals to drive a wedge between them and their families and communities. It is vital that school staff can recognise those vulnerabilities.
1.21. Staff will maintain and apply a good understanding of the relevant guidance to prevent pupils from becoming involved in terrorism.
1.22. The school will monitor its RE curriculum and assembly policy to ensure that they are used to promote community cohesion and tolerance of different faiths and beliefs.
1.23. Senior leaders will raise awareness within the school about the safeguarding processes relating to protecting pupils from radicalisation and involvement in terrorism.

Appendix Two : **Somerville Primary School Agreed Staff Code of Conduct to promote digital safety and responsible use**

To ensure that members of staff are fully aware of their professional responsibilities when using information systems and when communicating with pupils, they are asked to sign this code of conduct. Members of staff should consult the school's digital safety policy for further information and clarification.

- I understand that it is a criminal offence to use a school ICT system for a purpose not permitted by its owner. This school expects that all activity should be related to a professional use.
- I appreciate that ICT includes a wide range of systems, including mobile phones, tablet computers, digital cameras, email, social networking and that ICT use may also include personal ICT devices when used for school business. It is my responsibility to ensure that I do not store any inappropriate material on these devices in school.
- I understand that school information systems may not be used for private purposes without specific permission from the head teacher.
- I understand that my use of school information systems, Internet and email may be monitored and recorded to ensure policy compliance. This is managed by EXA internet filtering.
- I will respect system security and I will not disclose any password or security information to anyone other than an authorised system manager.
- I will not install any software or hardware without permission.
- I will ensure that personal data is stored securely and is used appropriately, whether in school, taken off the school premises or accessed remotely.
- I will respect copyright and intellectual property rights.
- I will report any incidents of concern regarding children's safety to the digital safety co-ordinator (head teacher) or the designated Child Protection Coordinator.
- I will ensure that electronic communications with pupils and parents including email, IM and social networking are compatible with my professional role and that messages cannot be misunderstood or misinterpreted.
- I will promote digital safety with students in my care and will help them to develop a responsible attitude to system use, communications and publishing.
- I am aware that I cannot use personal devices or mobile networks to access inappropriate content at school

The school may exercise its right to monitor the use of the school's information systems and Internet access, to intercept e-mail and to delete inappropriate materials where it believes unauthorised use of the school's information system may be taking place, or the system may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound.

I have read, understood and accept the Staff Code of Conduct for ICT.

Signed:_____ Date: _____

THINK THEN CLICK

Appendix Four – **Permission Letter for Network and Internet Use**

Somerville Primary School

Digital Safety Rules

Consent Form

All pupils use computer facilities including Internet access as an essential part of learning, as required by the National Curriculum. Both pupils and their parents/carers are asked to sign to show that the digital safety Rules have been understood and agreed.

Our digital safety policy is available from the school office and is published on the school's website.

Pupil:	***Year Group:***

Pupil's Agreement

- I have read and I understand the school digital safety Rules.
- I will use the computer, network, mobile phones, Internet access and other new technologies in a responsible way at all times.
- I know that network and Internet access may be monitored.

Signed:	***Date:***

Parent's Consent for Web Publication of Work and Photographs

I agree that my son/daughter's work may be electronically published. I also agree that appropriate images and video that include my son/daughter may be published subject to the school rule that photographs will not be accompanied by pupil names.

Parent's Consent for Internet Access

I have read and understood the school digital safety rules and give permission for my son / daughter to access the Internet. I understand that the school will take all reasonable precautions to ensure that pupils cannot access inappropriate materials but I appreciate that this is a difficult task.

I understand that the school cannot be held responsible for the content of materials accessed through the Internet. I agree that the school is not liable for any damages arising from use of the Internet facilities.

Signed:	***Date:***

Please print name:

Please complete, sign and return to the School Office

Appendix Five: **Consent Form for Visiting Adults Using our Network and Internet Access**

All adults have to responsible when using information systems. As visitors to schools, adults have to be aware that their activities must be related to education or their role within the school. In cases where the school feels that either their pupils or staff have been placed at risk, this could lead to the incident being investigated, please consult the school's digital safety policy for further information and clarification. This is available through the school office or the school's website.

- I understand that it is a criminal offence to use a school ICT system for a purpose not permitted by its owner. This school expects that all activity should be related to a professional and educational use.
- I appreciate that ICT includes a wide range of systems, including mobile phones, PDAs, digital cameras, email, social networking and that ICT use may also include personal ICT devices when used for school business.
- It is my responsibility to ensure that I do not store any inappropriate material on these devices in school.
- I understand that school information systems may not be used for private purposes without specific permission from the head teacher.
- I understand that my use of school information systems, Internet and email may be monitored and recorded to ensure policy compliance.
- I will respect system security and I will not disclose any password or security information to anyone other than an authorised system manager.
- I will not install any software or hardware without permission.
- I will ensure that no files are removed from the school's network without the express permission of a senior member of the school's staff.
- I will respect copyright and intellectual property rights.
- I will report any incidents of concern regarding children's safety to the Headteacher.
- I will ensure that all e-mail communication is appropriate.
- I will not access any inappropriate websites including social networking sites.
- I am aware that I cannot use personal devices or mobile networks to access inappropriate content at school.

The school may exercise its right to monitor the use of the school's information systems and Internet access, to intercept e-mail and to delete inappropriate materials where it believes unauthorised use of the school's information system may be taking place, or the system may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound.

I have read, understood and accept the Visitor's Code of Conduct for ICT.

Signed:_____ Date: _____

Appendix Six – Mobile Phone Policy

This policy applies to all individuals who have access to personal or work-related mobile phones on site. This includes staff, volunteers, children, young people, parents/ carers, visitors and community users. Policy applies to school and OTIS club staff.

Introduction:

Mobile phone technology has advanced significantly over the last few years - and it continues to evolve. Wireless connections in particular have extended the capabilities of mobile phones, enabling access to a wide range of new content and services globally. Many phones now offer Internet and email access, alongside the most often standard functions of messaging, camera, video and sound recording.

Mobile phones, alongside other forms of technology are changing the way and speed in which we communicate. They can provide security and reassurance. However, there are also associated risks.

Children and young people need to understand these risks in order to help them develop appropriate strategies for keeping themselves safe. As with e-safety issues generally, risks to children and young people can be broadly categorised under the headings of content, contact and conduct and managed by reducing availability, restricting access and increasing resilience.

Aim

The aim of the Mobile Phone Policy is to promote safe and appropriate practice through establishing clear and robust acceptable use guidelines for staff, visitors and children. This is achieved through balancing protection against potential misuse with the recognition that mobile phones are effective communication tools - which in turn can contribute to safeguarding practice and protection.

Policy

It is recognised that it is the enhanced functions of many mobile phones that cause the most concern, and which are most susceptible to misuse. Misuse includes:

- taking and distribution of indecent images,
- exploitation and exposure to emotional harm through being exposed to inappropriate content
- bullying through sharing content, images or videos.

It is also recognised that mobile phones can cause an unnecessary distraction during the working day and can be intrusive when used in the company of others. When mobiles phones are misused it can impact on an individual's dignity, privacy and right to confidentiality. Such concerns are not exclusive to children and young people; hence there is a duty to protect the needs and vulnerabilities of adults and visitors.

School's Expectations

Staff:

- Staff must only use mobile phones for personal use in office areas or staff room.
- Mobile phones must only be used in the staff room or outside of school hours and during lunch break. Only exception to this is senior, pastoral and site staff who are on call for work purposes.
- This includes:
    - Executive Head Teacher
    - Deputy Head Teacher
    - Assistant head Teachers
    - Business Manager
    - Site Manager
    - Assistant Site Manager
    - Learning Mentors (when they are working off site)
    - OTIS Club Manager (or deputising member of staff)
    - Technician
- Staff using mobile phones for work must avoid unnecessary use in the vicinity of children. An example of this could be the caretaker, site manager or a senior member of staff being contacted.
- Staff must not take images of children or store any data relating to children on their mobile phones.
- Staff, Volunteers and trainee teachers are not permitted to use their own personal phones for contacting children, young people and their families within or outside of the setting unless authorised by a member of the SMT.

- Staff should not access content that it is not suitable for professional use during working hours on whilst on school site. This includes social networking, pornography, inappropriate websites, dating websites etc.
- During school trips staff must only use phones for business reasons around children. They may need to be turned on for emergency contact needs.
- During residential trips staff will use mobile phones to contact families but must do this is an area away from children. Privacy of room, quiet space etc.
- Personal calls are not permitted to be made on the work mobile, other than in agreed exceptional circumstances. On residential strips, staff would do this as part of a designated break.
- If any practitioner is required to drive in a working capacity, and has responsibility for the work mobile, the phone must be switched off whilst driving. It is strongly recommend that practitioners follow the same procedures regarding their own personal mobile phones. Under no circumstances should practitioners drive whilst taking a phone call. This also applies to hands-free and wireless connections, which are considered a distraction rather than a safer alternative.
- Staff should ensure that their mobile phones are locked away safely if in school. They can be left at the office for safe storage. To protect themselves, staff should have their phone password protected.
- As well as safeguarding children and avoiding any unnecessary disruptions during the day, this procedure also aims to protect staff against any unfounded allegations.
- Staff who need to be available for emergency contact should give the school's phone number for contact during working hours. All phones are manned during the working day between 8.45-3.45pm. After this staff not supervising children may need to have their phones switched onto vibrate for emergency contact. OTIS Club should be available from 7.45am to 5.45pm.

Visitors:

- Parents/Visitors cannot use mobile phones on premises.
- Photographs can only be taken at authorised events such as carol concerts, performances etc. Parents have signed consent forms accepting their responsibility to use any images for personal use and not to share on any social networking sites.
- Other professionals must not use mobile phones in the immediate vicinity of children. We recognise that contractors, IT technicians will need access to mobile phones. They will be directed to office or staffroom areas.
- Professionals making or receiving work calls must do so in the office or staff room areas.
- Visitors should not access content that it is not suitable for professional use whilst on school site. This includes social networking, pornography, inappropriate websites, dating websites etc.
- During school trips volunteers must have mobile phones switched off.

Visitors who don't follow this code may be asked to leave the premises. They may not be allowed to return.

Children:

- Children are never allowed to use mobile phones on school site
- Children can bring phones into school in years 5 and 6 but must follow the following protocol:
  i. Phones must be turned off before they enter the premises
  ii. Phones must be placed in the school office during registration or upon entry to the classroom. Phones remain there until the end of the school day.
  iii. Phones should be collected at the end of the day and put in their bag/pocket.
  iv. Phones cannot be turned on until children leave the premises (playground).

Under no circumstances is any child permitted to take images or make recordings on a mobile phone.

Children cannot bring phones on school trip or residential visits.

Children not following these safety guidelines will:

- Have their phone removed and placed at the school office. It must be collected by an adult from here.
- If a second offence occurs in the calendar year, they will have their phones removed and left with a senior member of staff. They will also lose the privilege of being allowed a mobile phone for the rest of that year.

Appendix Seven–Social Media Policy

1 **POLICY STATEMENT**

1.1The internet and use of apps provides opportunities to participate in interactive discussions and the sharing of information using a wide variety of social media such as Facebook, Twitter, Istagram, blogs and wikis. However, employees' use of social media can pose risk to the School's confidential and proprietary information, and reputation.

1.2To minimise these risks and to ensure that the School's IT resources and communications systems are used only for appropriate purposes, the School expects employees to adhere to this policy. Policy will be reviewed every two years and shared with staff.

1.3This policy does not form part of any employee's contract of employment and it may be amended at any time.

2 **WHO IS COVERED BY THIS POLICY?**

2.1This policy covers all individuals working at all levels and grades throughout the School, including part time and fixed term employees, casual staff, agency staff and volunteers (collectively referred to as **staff** in this policy).

2.2Third parties who have access to the School's electronic communication systems and equipment are also required to comply with policy.

3 **SCOPE AND PURPOSE OF THE POLICY**

3.1This policy deals with the use of all forms of social media, including Facebook, Instagram, LinkedIn, Twitter, Wikipedia, all other social networking sites, and all other internet postings, including blogs.

3.2It applies to the use of social media for both professional and personal purposes, whether during work hours or otherwise. The policy applies regardless of whether the social media is accessed using the School's IT facilities and equipment or equipment belonging to members of staff.

3.3Breach of this policy may result in disciplinary action up to and including dismissal.

3.4Disciplinary action may be taken regardless of whether the breach is committed during working hours, and regardless of whether the School's equipment or facilities are used for the purpose of committing the breach.

3.5Any member of staff suspected of committing a breach of this policy will be required to co-operate with any investigation that may follow, which may involve handing over relevant passwords and login details for school provided hardware, software and remote access.

3.6Staff will be required to remove internet postings which are deemed to constitute a breach of this policy. Failure to comply with such a request may in itself result in disciplinary action.

4 **PERSONNEL RESPONSIBLE FOR IMPLEMENTATION OF THE POLICY**

4.1The Board of Governors has overall responsibility for the effective operation of this policy, but has delegated day-to-day responsibility for its operation to the Head Teacher. Responsibility for monitoring and reviewing the operation of this policy and making recommendations for change to minimise risks also lies with the Head Teacher.

4.2All managers have a specific responsibility for operating within the boundaries of this policy, ensuring that all staff understand the standards of behaviour expected of them and taking action when behaviour falls below its requirements. Training will, if required, be provided to facilitate this.

4.3All staff are responsible for the success of this policy and should ensure that they take the time to read and understand it. Any misuse of social media should be reported to the Head Teacher and the Board of Governors.

4.4Questions regarding the content or application of this policy should be directed to the Head Teacher.

5 COMPLIANCE WITH RELATED POLICIES AND AGREEMENTS

5.1 Social media should never be used in a way that breaches any the other policies of the School. If an internet post would breach any of the School's policies in another forum, it will also breach them in an online forum. Staff are prohibited from using social media to:

5.1.1 breach any obligations the school has in relation to the duty of confidentiality to its staff and pupils, both past and present;

5.1.2 breach our disciplinary policy;

5.1.3 defame or disparage the School its staff, pupils and third parties connected with the school, for example pupils' parents;

5.1.4 breach the school's anti-harassment and bullying policy;

5.1.5 breach the school's equal opportunities policy;

5.1.6 breach the data protection policy;

5.1.7 breach any other laws or ethical standard (for example, never use social media in a false or misleading way, such as by claiming to be someone other than yourself or by making misleading statements).

5.2 Staff should never provide references for other individuals on social or professional networking sites. Such references, whether positive or negative, can be attributed to the School and create legal liability for the School accordingly and the individual providing the reference.

5.3 Employees who breach any of the above policies will be subject to disciplinary action up to and including termination of employment.

5.4 If we have authorised use using apps such as twitter, see-saw etc staff will be sharing good news on behalf of the school. If any inappropriate content is posted they should report that to the provider (Twitter etc) and to the head teacher. They do not need to comment themselves.

5.5 Staff may support PTA groups on social media but should not comment on school business, other staff or children.

6 PERSONAL USE OF SOCIAL MEDIA

Personal use of social media is never permitted during working time or by means of the School's computers, networks and other IT resources and communications systems.

7 MONITORING

7.1 In light of the exemption of personal use of social media during working time, the contents of the School's IT resources and communications systems are the School's property. Staff should therefore have no expectation of privacy in any messages, files, data, document or social media post conversation or message transmitted to, received or printed from, or stored or recorded on the School's electronic information and communications systems.

7.2 The Board of Governors of the School reserve the right to monitor, intercept and review, without further notice, staff activities using the School's IT and communication systems, including but not limited to social media postings and activities to ensure that rules are being complied with, and for legitimate business purposes. You consent to such monitoring by your use of such resources and systems.

7.3 Staff should not use the School's IT resources and communications systems for any matter that he/she wishes to be kept private or confidential.

8 BUSINESS USE OF SOCIAL MEDIA

8.1 It is unlikely that any member of staff will be required to speak on behalf of the School in a social media environment, but in the event that you are, you must still seek the approval for such

communication from the Head Teacher who may require you to undergo training before you do so and impose certain requirements and restrictions with regard to your activities.

8.2 Likewise, if you are contacted for comments about the School for publication anywhere, including in any social media outlet, you should direct the enquiry to the Head Teacher and do not respond without written approval.

8.3 The use of social media for business is subject to the remainder of this policy.

9 RECRUITMENT

We may use internet searches to perform due diligence on candidates in the course of recruitment. Where the School does this, it will act in accordance with its data protection and equal opportunities obligations.

10 RESPONSIBLE USE OF SOCIAL MEDIA

10.1 Staff have to accept that their professional responsibilities trump that of their personal considerations. **Staff should not have friends/link on social media who are parents at the school.** This ensures that there is no abuse of privacy either directly or indirectly (friends of friends links etc).

10.2 **Staff must not have social media links with ex-pupils until they are over aged 21**. This prevents abuse of power situations with minors.

10.3 The following sections of the policy provide staff with common-sense guidelines and recommendations for using social media responsibly and safely.

10.4 Protecting the School's reputation:

10.4.1 Staff must not post disparaging or defamatory statement about:

10.4.1.1 the School as an organisation;

10.4.1.2 members of staff or pupils;

10.4.1.3 third parties connected with the School, e.g. parents

10.5 Staff should also avoid social media communications that might be misconstrued in a way that could damage the School's reputation.

10.6 Staff should make it clear in social media postings that they are speaking on their own behalf, and not on behalf of the School or The Board of Governors A way to achieve this would be writing in the "first person".

10.7 If you disclose your affiliation with the School you should state that your views do not represent those of your employer. For example, you could state, "the views in this posting do not represent the views of my employer".

10.8 Staff are personally responsible for what they communicate in social media.

10.9 Staff should ensure that the content of their postings is consistent with professional image as an employee of the School.

10.10 If you are uncertain or concerned about the appropriateness of any statement or posting, you should refrain from making the communication until you discuss it with the Head Teacher.

10.11 If you see content in social media that disparages or reflects poorly on the School or any member of staff, you should contact the Head Teacher on behalf of the Board of Governors.

10.12 Staff should not do anything to jeopardise confidential information of the School, its staff or pupils through use of social media.

10.13 Staff should avoid misappropriating or infringing the intellectual property of other companies and individuals as this may create liability for the School and the individual concerned.

10.14 Staff should not post anything that colleagues would find offensive, including discriminatory comments, insults or obscenity.

10.15 Staff should not post anything related to your colleagues or pupils without their or their parents' written permission and consent.