Attleborough Primary School

Online Safety Policy

Date: January 2020

Review: January 2022

Contents:

Statement of intent

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 and are provided with guidance and a range of strategies on how to act if they see, hear or read something that makes them feel uncomfortable.

As a result, designing and implementing an Online safety Policy demands the involvement of a wide range of interest groups: the governors, headteacher, SLT, SENCO, DSL, classroom teachers, support staff, young people or parents, LA personnel, internet service providers (ISP), and regional broadband consortia, working closely with ISPs on network security measures.

Online safety is a child protection issue, and indeed it should not be managed primarily by the ICT team. It should be an extension of general safeguarding and led by the same people, so that, for instance, cyber bullying is considered alongside real-world bullying.

An Online safety Policy should:

- Allow young people to develop their own protection strategies for when adult supervision and technological protection are not available.
- Give information on where to seek help and how to report incidents.
- Help young people understand that they are not accountable for the actions that others may force upon them but that there are sanctions that the school will impose if they act inappropriately when online.
- Provide guidelines for parents and others on safe practice.
- Ensure you regularly monitor and review your policies with stakeholders.
- Ensure technological solutions are regularly reviewed and updated to ensure maintenance of an effective online safety programme.

Above all, online safety education should be a continuing feature of both staff development and young people's educational lifelong learning.

The purpose of this policy is to:

- Set out the key principles expected of all members of the school community at school with respect to the use of ICT-based technologies.
- Safeguard and protect the children and staff of the school.
- Assist 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.

- Set clear expectations of behaviour and/or codes of practice relevant to responsible use of the internet for educational, personal or recreational use Have 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.
- Minimise the risk of misplaced or malicious allegations made against adults who work with pupil.

1. Teaching and learning

Why the internet and digital communications are important

1.1. The internet is 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.

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

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

1.4. Staff model safe and responsible behaviour in their use of technology during lessons.

1.5. Teachers remind pupils about their responsibilities through an end-user Pupil Acceptable Use Agreement which every pupil will sign when they log on to the school network.

Internet use will enhance learning

1.6. The school internet access will be designed expressly for pupil use and will include filtering appropriate to the age of pupils.

1.7. Pupils will be taught what internet use is acceptable and what is not and given clear objectives for internet use.

1.8. Pupils will be educated in the effective use of the internet in research, including the skills of knowledge location, retrieval and evaluation.

1.9. Pupils will be shown how to publish and present information to a wider audience.

Pupils will be taught how to evaluate internet content

1.10. The school will ensure that the use of internet derived materials by staff and pupils complies with copyright law.

1.11. Pupils will be taught the importance of cross-checking information before accepting its accuracy.

1.12. Pupils will be taught how to report unpleasant internet content to the online safety coordinator (the safeguarding team). This can be done anonymously, or in person, and will be treated in confidence.

1.13. The 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 their age and experience

2. Managing internet access

Information system security

2.1. School ICT systems security will be reviewed regularly.

2.2. Virus protection will be updated regularly.

2.3. Security strategies will be discussed with the LA.

Email

2.4. Pupils and staff may only use approved email accounts on the school system.

2.5. Pupils must immediately tell a teacher if they receive an offensive email.

2.6. In email communication, pupils must not reveal their personal details or those of others or arrange to meet anyone without specific permission.

2.7. Incoming emails will be treated as suspicious and attachments not opened unless the author is known.

2.8. The school:

- Provides staff with an email account for their professional use (Microsoft 365) and makes clear personal email should be through a separate account.
- Does not publish personal email addresses of pupils or staff on the school website.
- Will contact the police if one of our staff or pupils receives an email that it considers is particularly disturbing or breaks the law.
- Will ensure that email accounts are maintained and up-to-date.
- Reports messages relating to or in support of illegal activities to the relevant authority and if necessary to the police.
- Knows that spam, phishing and virus attachments can make emails dangerous.

Published content and the school website

2.9. Staff or pupil personal contact information will not be published. The contact details given online should be the school office.

2.10. The headteacher will take overall editorial responsibility and ensure that content is accurate and appropriate, and the quality of presentation is maintained.

2.11. Uploading of information is restricted to our website authorisers.

2.12. The school website complies with the following statutory DfE guidelines for publications: What maintained schools must publish online

2.13. Most material is the school's own work; where others' work is published or linked to, we credit the sources used and state clearly the author's identity or status.

2.14. The point of contact on the website is the school address and telephone number. The school uses a general email contact address, e.g. office@attleborough-pri.norfolk.sch.uk. Home information or individual email identities will not be published.

2.15. Photographs published on the web do not have full names attached.

2.16. The school does not use pupils' names when saving images in the file names or in the tags when publishing to the school website.

2.17. The school expects teachers using school approved blogs or wikis to password protect them and run from the school website.

Publishing pupils' images and work

2.18. Photographs that include pupils will be selected carefully so that individual pupils cannot be identified, or their image misused. The school will consider using group photographs rather than full-face photos of individual children.

2.19. Pupils' full names will not be used anywhere on a school website or other online space, particularly in association with photographs.

2.20. Written permission from parents will be obtained before photographs of pupils are published on the school website.

2.21. Work can only be published with the permission of the pupil and parents.

2.22. Pupil image file names will not refer to the pupil by name.

2.23. Parents should be clearly informed of the school policy on image taking and publishing, both on school and independent electronic repositories.

2.24. The school gains parental permission for use of digital photographs or video involving their child as part of the school agreement form when their child joins the school.

2.25. The school does not identify pupils in online photographic materials or include the full names of pupils in the credits of any published school produced video materials/DVDs.

2.26. Staff sign the school's Staff, Governor and Visitor Acceptable Use Agreement, and this includes a clause on the use of mobile phones/personal equipment for taking pictures of pupils.

2.27. If specific pupil photos (not group photos) are used on the school website or in other high profile publications, the school will obtain parental permission.

2.28. The school blocks/filters access to social networking sites or newsgroups unless there is a specific approved educational purpose.

2.29. Pupils are taught about how images can be manipulated in their online safety education programme and to consider how to publish for a wide range of audiences which might include governors, parents or younger children as part of their ICT scheme of work.

2.30. Pupils are advised to be very careful about placing any personal photos on any 'social' online network space. They are taught to understand the need to maintain privacy settings so as not to make public, personal information.

2.31. Pupils are taught that they should not post images or videos of others without their permission. The school teaches them about the risks associated with providing information with images (including the name of the file), that reveals the identity of others and their location, such as house number, street name or school. The school teaches them about the need to keep their data secure and what to do if they are subject to bullying or abuse.

3. Social Networking and Personal Publishing

Information system security

3.1 The headteacher is responsible for:

- Promoting safer working practices and standards with regards to the use of social media.
- Establishing clear expectations of behaviour for social media use.
- Implementing appropriate sanctions and disciplinary methods where there is a breach of this policy.
- Taking steps to minimise the amount of misplaced or malicious allegations in relation to social media use.
- Working alongside the online safety officer and data protection officer (DPO) to ensure appropriate security measures are implemented and compliance with the GDPR.

3.2 Staff members are responsible for:

- Adhering to the principles outlined in this policy and the Staff, Governor and Visitor Acceptable Use Agreement

- Ensuring pupils adhere to the principles outlined in this policy and that it is implemented fairly and consistently in the classroom.
- Reporting any social media misuse by staff, pupils or parents to the headteacher immediately.
- Attending any training on social media use offered by the school.

3.3 Parents are responsible for:

- Adhering to the principles outlined in this policy
- Taking appropriate responsibility for their use of social media and the influence on their children at home.
- Promoting safe social media behaviour for both themselves and their children.

3.4 Pupils are responsible for:

- Adhering to the principles outlined in this policy and the Pupil ICT Code of Conduct.
- Ensuring they understand how to use social media appropriately and stay safe online.

Definitions

3.3 For the purpose of this policy, the school defines **"social media"** as any online platform that offers real-time interaction between the user and other individuals or groups including, but not limited to, the following:

- Blogs
- Online discussion forums, such as netmums.com
- Collaborative spaces, such as Facebook
- Media-sharing devices, such as YouTube
- 'Micro-blogging' applications, such as Twitter

3.4 For the purpose of this policy, **"cyber bullying"** is defined as any social media or communication technology intentionally used to bully an individual or group, including the posting or sharing of messages, images or videos.

3.5 For the purpose of this policy, **"members of the school community"** are defined as any teacher, member of support staff, pupil, parent of a pupil, governor or ex-pupil.

Data protection principles

3.6 The school will obtain consent from pupils and parents the Images and Videos Parental Consent Form, which will confirm whether or not consent is given for posting images and videos of a pupil on social media platforms. The consent will be valid for the **entire academic year**.

3.7 A record of consent is maintained throughout the academic year, which details the pupils for whom consent has been provided. The DPO is responsible for ensuring this consent record remains up-to-date.

3.8 Parents and pupils are able to withdraw or amend their consent at any time. To do so, parents and pupils must inform the school in writing.

3.9 Where parents or pupils withdraw or amend their consent, it will not affect the processing of any images or videos prior to when consent was withdrawn or amended. Processing will cease in line with parents' and pupils' requirements following this.

3.10 The school will only post images and videos of pupils for whom consent has been received.

3.11 Only school-owned devices will be used to take images and videos of the school community, which have been pre-approved for use.

3.12 When posting images and videos of pupils, the school will apply data minimisation techniques, such as pseudonymisation (blurring a photograph), to reduce the risk of a pupil being identified.

3.13 The school will not post pupils' personal details on social media platforms.

3.14 Pupils' full names will never be used alongside any videos or images in which they are present.

3.15 Only appropriate images and videos of pupils will be posted in which they are suitably dressed, i.e. it would not be suitable to display an image of a pupil in swimwear.

3.16 When posting on social media, the school will use group or class images or videos with general labels, e.g. 'sports day'.

3.17 Before posting on social media, staff will:

- Refer to the consent record log to ensure consent has been received for that pupil and for the exact processing activities required.
- Ensure that there is no additional identifying information relating to a pupil.

3.18 Any breaches of the data protection principles will be handled in accordance with the school's **Data and E-Security Breach Prevention and Management Plan**.

3.19 Consent provided for the use of images and videos only applies to school accounts – staff, pupils and parents are not permitted to post any imagery or videos on personal accounts.

Data protection principles

School accounts

3.20 School social media passwords are kept in the office – these are not shared with any unauthorised persons, including pupils, unless otherwise permitted by the headteacher.

3.21 Staff will ensure any posts are positive in nature and relevant to pupils, the work of staff, the school or any achievements.

3.22 Staff will ensure a colleague has checked the content before anything is posted on social media.

3.23 Staff will adhere to the data protection principles outlined in this policy at all times.

3.24 Staff will not post any content online which is damaging to the school or any of its staff or pupils.

3.25 If inappropriate content is accessed online, a report form will be completed and passed on to the online safety officer (The safeguarding team). The online safety officer retains the right to monitor staff members' internet usage in line with the **Data and E-Security Breach Prevention and Management Plan**.

Personal accounts

3.30 Staff members will not access social media platforms during lesson times.

3.31 Staff members will not use any school-owned mobile devices to access personal accounts, unless it is beneficial to the material being taught – prior permission will be sought from the headteacher.

3.32 Staff members are permitted to use social media during break times.

3.33 Staff are not permitted to use the school's WiFi network to access personal accounts, unless otherwise permitted by the headteacher.

3.34 Staff will avoid using social media in front of pupils.

3.35 Staff will not "friend" or otherwise contact pupils or parents through their personal social media accounts.

3.36 If pupils or parents attempt to "friend" a staff member they will report this to the headteacher.

3.37 Staff members will not provide their home address, phone number, mobile number, social networking details or email addresses to pupils or parents – any contact with pupils or parents will be done through authorised school contact channels.

3.38 Staff members will ensure the necessary privacy controls are applied to personal accounts.

3.39 Staff members will avoid identifying themselves as an employee of Attleborough Primary School on their personal social media accounts.

3.40 No staff member will post any content online that is damaging to the school or any of its staff or pupils.

3.41 Where staff members use social media in a personal capacity, they will ensure it is clear that views are personal and are not that of Attleborough Primary School.

3.42 Staff members will not post any information which could identify a pupil, class or the school – this includes any images, videos and personal information.

3.43 Staff will not take any posts, images or videos from social media that belong to the school for their own personal use.

3.44 Staff members will not post anonymously or under an alias to evade the guidance given in this policy.

3.45 Breaches of this policy by members of staff will be taken seriously, and in the event of illegal, defamatory or discriminatory content, could lead to prosecution, disciplinary action or dismissal.

3.46 Members of staff will be aware that if their out-of-work activity brings the school into disrepute, disciplinary action will be taken.

3.47 Members of staff will regularly check their online presence for negative content via search engines.

3.48 Attempts to bully, coerce or manipulate members of the school community via social media by members of staff will be dealt with as a disciplinary matter.

3.49 Members of staff will not leave a computer or other device logged in when away from their desk or save passwords.

3.50 Staff members will use their school email address for school business and personal email address for their private correspondence; the two should not be mixed.

Social media use – pupils and parents

3.51 Pupils will not access social media during lesson time, unless it is part of a curriculum activity.

3.52 Pupils and parents will not attempt to “friend” or otherwise contact members of staff through their personal social media accounts. Pupils and parents are only permitted to be affiliates of school social media accounts.

3.53 Where a pupil or parent attempts to “friend” a staff member on their personal account, it will be reported to the headteacher.

3.54 Pupils and parents will not post anonymously or under an alias to evade the guidance given in this policy.

3.55 Pupils and parents will not post any content online which is damaging to the school or any of its staff or pupils.

3.56 Pupils are instructed not to sign up to any social media sites that have an age restriction above the pupil's age.

3.57 If inappropriate content is accessed online on school premises, it will be reported to a teacher.

3.58 Pupils are not permitted to use the school's WiFi network to access any social media platforms unless prior permission has been sought from the headeacher.

3.59 Parents are not permitted to use the school's WiFi network to access any social media platforms on personal devices.

3.60 Breaches of this policy will be taken seriously, and in the event of illegal, defamatory or discriminatory content could lead to prosecution, or exclusion

Blocked content

3.62 In accordance with the school's **Data and E-Security Breach Prevention and Management Plan**, the online safety officer installs firewalls on the school's network to prevent access to certain websites. The following social media websites are not accessible to students on the school's network:

- Twitter
- Facebook
- Instagram
- YouTube

3.63 Attempts made to circumvent the network's firewalls will result in a ban from using school computing equipment, other than with close supervision.

3.64 Inappropriate content accessed on the school's computers will be reported to the online safety officer (The safeguarding team) so that the site can be blocked.

3.65 The online safety officer retains the right to monitor staff and pupil access to websites when using the school's network and on school-owned devices.

4. Managing emerging technologies

4.1. Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.

4.2. The SLT 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.

4.3. Mobile phones will not be used during school time. The sending of abusive or inappropriate text messages or files by Bluetooth or any other means is forbidden.

4.4. The use by pupils of cameras in mobile phones will be kept under review.

4.5. Staff will not use personal mobile phones to communicate with children or use them to capture images of them.

Protecting personal data

4.6. Personal data will be recorded, processed, transferred and made available according to the GDPR and the Data Protection Act 2018.

5. Policy Decisions

Authorising internet access

5.1. All staff will read and sign the Staff, Governor and Visitor Acceptable Use Agreement before using any school ICT resource.

5.2. The school will maintain a current record of all staff and pupils who are granted access to school ICT systems.

5.3. At EYFS and KS1, access to the internet will be by adult demonstration with directly supervised access to specific, approved online materials.

5.4. Any person not directly employed by the school will be asked to sign the Staff, Governor and Visitor Acceptable Use Agreement before being allowed to access the internet from the school site.

Assessing risks

5.5. 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 LA can accept liability for any material accessed, or any consequences of internet access.

5.6. The school should audit ICT use to establish if the Online safety Policy is adequate and that the implementation of the Online safety Policy is appropriate and effective.

Handling online safety complaints

5.7. Complaints of internet misuse will be dealt with by a senior member of staff.

5.8. Any complaint about staff misuse must be referred to the headteacher.

5.9. Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.

5.10. Pupils and parents will be informed of the complaints procedure (see school's complaints policy)

5.11. Pupils and parents will be informed of the consequences for pupils misusing the internet.

5.12. Discussions will be held with the police youth crime reduction officer to establish procedures for handling potentially illegal issues.

6. Pupil online safety curriculum

Teaching and learning

6.1. This 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 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.

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

6.3. The school will remind pupils about their responsibilities through a Pupil Acceptable Use Agreement/ICT code of conduct which every pupil will sign.

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

Online risks

6.5. The 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

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

6.7. 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.

6.8. Through the PSHE curriculum, children are taught to tell a responsible adult if they receive inappropriate, abusive or harmful emails or text messages.

6.9. Posters providing information about how to get help from Childline, ThinkUKnow and the NSPCC are displayed in classrooms and along the corridors of the school.

6.10. 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.

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

6.12. All incidents of cyber bullying reported to the school will be recorded.

Sexual exploitation/sexting

6.13. Sexting between pupils will be managed through our anti-bullying and confiscation procedures.

6.14. All staff are made aware of the indicators of sexual exploitation and all concerns are reported immediately to the DSL.

6.15. There are clear procedures in place to support anyone in the school community affected by sexting.

6.16. All incidents of sexting reported to the school will be recorded.

Radicalisation or extremism

6.17. Radicalisation refers to the process by which a person comes to support terrorism and forms of extremism leading to terrorism.

6.18. 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."

6.19. 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.

6.20. 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.

6.21. Staff will maintain and apply a good understanding of the relevant guidance to prevent pupils from becoming involved in terrorism.

6.22. 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.

6.23. Senior leaders will raise awareness within the school about the safeguarding processes relating to protecting pupils from radicalisation and involvement in terrorism.

7. Communications policy

Introducing the Online safety Policy to pupils

7.1. Online safety rules and guidance posers will be displayed in classrooms and discussed with pupils regularly.

7.2. Pupils will be informed that network and internet use will be monitored and appropriately followed up.

7.3. A programme of training in online safety will be developed by the computing coordinator, PSHE coordinator and DSL.

7.4. Safety training will be embedded within the computing and PSHE schemes of work in line with national curriculum expectations.

Staff and the online safety policy

7.5. All staff will be given the school Online safety Policy and have its importance explained.

7.6. Staff must be informed that network and internet traffic can be monitored and traced to the individual user.

7.7. Staff that manage filtering systems or monitor ICT use will be supervised by senior management and work to clear procedures for reporting issues.

Enlisting parents' support

- Parents' attention will be drawn to the school Online safety Policy in an online safety leaflet, newsletters and on the school website.
- The school will ask all new parents to sign the parent/pupil agreement when they register their child with the school.

Useful Resources for Teachers and Parents

Resource	Website
Child Exploitation and Online Protection Centre	www.ceop.gov.uk/
Childnet	www.childnet-int.org/
Digizen	www.digizen.org/
Kidsmart	www.kidsmart.org.uk/
Think U Know	www.thinkuknow.co.uk/
Family Online Safety Institute	http://www.fosi.org
Internet Watch Foundation	www.iwf.org.uk
Internet Safety Zone	www.internetsafetyzone.com
Vodafone digital parenting	www.vodafone.com/content/digital-parenting.html
NSPCC - Share Aware	www.nspcc.org.uk/preventing-abuse/keeping-children-safe/share-aware
Parent Zone	www.theparentzone.co.uk/school

Staff, Governor and Visitor Acceptable Use Agreement

ICT and the related technologies, such as email, the internet and mobile devices, are an expected part of daily working life in school. This policy is to help ensure that all staff are aware of their professional responsibilities when using any form of ICT and to help keep staff, governors and visitors safe. All staff are expected to sign this agreement confirming their undertaking to adhere to its contents at all times. Any concerns or clarification should be discussed with the headteacher**.**

- I will only use the school's email, internet, learning platform and any related technologies for professional purposes or for uses deemed 'reasonable' by the headteacher or governing board.
- I will comply with the ICT system security and not disclose any passwords provided to me by the school or other related authorities.
- I will ensure that all electronic communications with pupils and staff are compatible with my professional role.
- I will not give out my personal details, such as mobile phone number or personal email address, to pupils.
- I will only use the approved email system for any communications with pupils, parents and other school-related activities.
- I will ensure that personal data (such as data held on the administration system) is kept secure and is used appropriately. Personal data can only be taken out of the school or accessed remotely when authorised by the headteacher or governing board and with appropriate levels of security in place.
- I will not install any hardware or software on school equipment without the permission of the headteacher.
- I will report any accidental access to inappropriate materials immediately to my line manager.
- I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.
- Images of pupils and/or staff will only be taken, stored and used for professional purposes in line with data protection policy and with written consent of the parent or staff member. Images will not be distributed outside the school network without the permission of the parent, member of staff or headteacher in line with data security policy.
- I understand that all my use of the Internet and other related technologies can be monitored and logged and can be made available to the headteacher.

- I will respect copyright and intellectual property rights.

    - I will ensure that my online activity, both in school and outside school, will not bring my professional role into disrepute. This includes ignoring invitations from pupils and parents to be part of their social networking site(s).

    - I will support and promote the school's Online safety Policy and help pupils to be safe and responsible in their use of ICT and related technologies.

User signature

I agree to follow this acceptable use policy and to support the safe use of ICT throughout the school.

Signature _____

Date _____

Full name _____ (Printed)

ICT Code of conduct for pupils

1. I should feel safe and enjoy being on the internet
2. I should be able to tell someone if something has worried me on the internet
3. I should not be bullied on the internet, and should not bully others
4. I should help my friends stay safe on the internet
5. I should be able to report anything that worries me on the internet
6. I should be able to talk and play on the internet with my friends
7. I shouldn't have to see unpleasant or hurtful things on the internet
8. I should know how to keep my personal information safe
9. I should be able to easily search the internet for information
10. I should learn how to stay safe on the internet

I agree to these statements

Name of child: ……

Parent Signature: ……