E-Safety Policy
Updated September 2016

Appendix

Safety Audit

This quick self-audit will help the senior leadership team assess whether the e-safety basics are in place.

Has the school an E-safety Policy that complies the latest guidance?	Yes
Date of lastest review:	September 2016
The Policy was agreed by governors on :	
The Policy is available for staff at:	Computing Folder
And for parents at:	School Website
The Designated Child Protection Coordinator is:	Alison Dale
The E-safety / COMPUTING Cordinator is:	John Broadbent
Has Esafety training been provided for staff?	Yes
Has Esafety training been provided for pupils?	Yes
Do parents sign & return • An agreement that their child will comply with the School Esafety rules? • The Acceptable User Policy (AUP) for pupils ? • An agreement that their children's work & pComputingures may be displaye on the internet.	 Yes Yes (Differentiated) Yes
Has the school got an AUP / Esafety Rules age appropriate for pupils?	Yes
Is the AUP / Essafety rules displayed in all rooms with computers?	Yes
Internet access is provided by an educational Internet service provider and complies with DfES requirements for safe and secure access?	Yes Bolton ICT
Has an ICT security audit been initiated by SMT, possibly using external expertise?	Yes (Deb Lyons)
Is personal data collected, stored and used according to the principles of Data Proctection Act?	Yes

Members of staff who have imputed directly with this policy	
Principal	Mrs D Murphy
Member of Senior Leadership Team	
Esafety / COMPUTING Coordinator	Mr J Broadbent
Designated Child Protection Coordinator	Mrs A Dale
Linked Governor	Mr A Morris
Member of TA staff	Miss C Diggle
School Council Representation (once a term one meeting to have an Esafety update Which they then in turn feedback to their peers)	Miss N Daisley

This policy outlines our purpose in providing e-mail and access to the Internet at **The Ferns Primary Academy** and explains how the academy is seeking to avoid the potential problems that unrestricted Internet access could give rise to. It is not the intention of the policy to be unnecessarily restrictive. The aim of the policy is to ensure there is a framework of control in place.

INTERNET ACCESS IN SCHOOL

Providing access to the Internet in school will raise educational standards and support the professional work of staff.

Teachers will have access to the Internet offering educational resources, news and current events they will also be able to communicate with the advisory and support services, professional associations and colleagues; exchange curriculum and administration data with the LA, DfES and our Academy sponsor.
The Internet is being used to enhance the school's management information and business administration systems.
Pupils will have access to the Internet offering educational resources, news and current events. There will be opportunities for discussion with experts in many fields and to communicate and exchange information with students and others world-wide.

All staff (including teachers, supply staff and classroom assistants) and any other adults involved in supervising children accessing the Internet will be provided with the School Internet Access Policy and will have its importance explained to them.

Parents will be drawn to the Policy by letter in our school prospectus and online within the ESafety section of the schools' web site.

USING E-MAIL

All staff are strongly advised **NOT** to use or share their personal email account for school and therefore are issued with their own professional email which they will use appropriately to communicate with colleagues, parents, pupils and schools external services.

Staff should be aware the internet traffic maybe monitored and traced to the individual device or login. Discretion and professional conduct is essential. All email and electronic communication can be monitored at all times and could be open to investigation should the need arise by the Head teacher with the support of Bolton Schools COMPUTING Unit (SCOMPUTING)

Pupils will learn how to use an age appropriate e-mail application

- Once they have been taught the Rules of Responsible Internet Use and agreed their Acceptable User Policy.
- Teachers will endeavour to ensure that these rules remain uppermost in the children's minds as they monitor children using e-mail;
- Pupils will not be permitted to use e-mail at school to arrange to meet someone.

INTERNET ACCESS AND HOME/SCHOOL LINKS

Parents will be informed in our school prospectus that pupils are provided with supervised Internet access as part of their lessons and are asked to provide written consent (They do not wish…) at the beginning of each academic year. We will keep parents in touch with future COMPUTING developments by newsletters the school web site and blog.

ESafety will be taught to all pupils either by a focus block of lessons and referred to then throughout the year and will be readdressed every year. Sessions will be taught using age appropriate resources and cover the following areas: Email, SMS Messaging, Social Networking and Cyber Bullying. All children within these sessions will agree to their own Acceptable Users Policy. A most important element of our AUP / Esafety Rules is that pupils will be taught to tell a teacher immediately if they encounter any material that makes them feel uncomfortable.

Esafety assemblies will be held throughout the year where appropriate.

If a reported incident arises, staff will log the event with the Esafety / ICT Co-ordinator, staff will be informed and if appropriate a letter will be sent home to inform parents and a discussion to take place with all parties.

New families entering the school during the academic year will be made aware of the SMART Rules available from www.childnet.com and will be briefed on Esafety and assigned a ICT buddy/ peer mentor.

Parents' attention will be drawn to the school Esafety policy in newsletters, school prospectus and on the school website / school blog. A series of parent workshops will be held throughout the year to support parents with e-safety and build strong partnership between parents, pupils and staff.

USING INFORMATION FROM THE INTERNET

We believe that, in order to use information from the Internet effectively, it is important for pupils to develop an understanding of the nature of the Internet and the information available on it. In particular, they should know that, unlike the school library for example, most of the information on the Internet is intended for an adult audience, much of the information on the Internet is not properly audited/edited and most of it is copyright.

- Pupils will be taught to expect a wider range of content, both in level and in audience, than is found in the school library or on TV;
- Teachers will ensure that pupils are aware of the need to validate information whenever possible before accepting it as true;
- When copying materials from the Web, pupils will be taught to observe copyright;
- Pupils will be made aware that the writer of an e-mail or the author of a web page may not be the person claimed.
- Pupils will be taught what Internet use is. The need for reliable information and given clear learning objectives for Internet use from the staff.
- Pupils will be educated in the effective use of Internet in research, including the skills of knowledge location, retrieval and evaluation appropriate to their age. In order to minimise the risk of children accessing harmful sites, staff to predetermine appropriate web links and add to a resource area the children can access.

If there is an incident in which a pupil is exposed to offensive or upsetting material, the school will wish to respond to the situation quickly and on a number of levels

- Staff will log the event with the Esafety / ICT Co-ordinator;
- A letter will be sent home to inform parents;
- Discussion to take place with all parties.

Serious incidents within school will be referred to the Child Protection Officer in consultation with the Head Teacher and the pupil's class teacher.

Pupils are expected to play their part in reducing the risk of viewing inappropriate material by obeying the AUP / Esafety Rules which have been designed to help protect them from exposure to Internet sites carrying offensive material. If pupils abuse the privileges of access to the Internet by failing to follow the rules they have been taught and rules set within the acceptable users' policy; then sanctions consistent with our School Behaviour Policy will be applied. This may involve informing the parents/carers and access to the Internet may be denied for a period of time.

MOBILE PHONES, DEVICES, AND CAMERAS

Some parents allow their children to have access to mobile telephones and digital cameras at home and in the community. There is normally no need for pupils to have a mobile phone or digital camera on school premises but we accept that there may be exceptional circumstances where parents see a need for their child to carry a mobile phone on their journey to and from school. In these exceptional circumstances parents must complete the

relevant form for their child to bring a mobile phone onto school premises. The pupil must comply with the requirements of this policy.

- Pupils will not be allowed to have mobile phones on school premises or to take them on visits or other school initiated activities without the permission of the Headteacher
- Mobile phones and cameras brought onto school premises or on activities or visits by pupils without permission will be confiscated and parents will be required to visit the school to have the phone returned to them in person
- Pupils who have been given permission to bring a mobile phone to school must switch it off and hand it in to the office on arrival and seek its return at the end of the school day

Volunteers, Visitors, Parents and Carers

- All home/school communication during the school day must be done through the school telephone system
- Pupils, parents or other adults must not take pictures or make video recordings with mobile phones or with any other cameras or devices on the school premises (including the field) without the Headteacher's permission
- Whilst on school premises or school visits, pupils and others may only use the internet via the school computer system. Mobile phones must never be used on school premises or on school activities to connect to the internet unless the Headteacher has given permission
- Where parents and carers are accompanying pupils on school trips, they should not use their devices to take photographs of children or access social networking
- Any cyber bullying of staff or pupils, in or out of school, must be reported and then investigated rigorously, in conjunction with any relevant authority including the police if appropriate

Staff and Governors

- Staff should have phones off or on silent away from view when in the vicinity of pupils
- Staff are not permitted to use mobile phones during teaching time, assemblies, on playground duty or while supervising children – with the exception of trips and visits where their use is permitted to facilitate the health and safety of the members of the party
- If photographs of pupils are required for display or curriculum evidence these may only be taken on a school camera
- Staff wishing to use their mobile telephones or check for messages during the school day should do so during a break period and take into consideration the location of where they are making the call – for example if a class is outside at break time and the classroom empty, this would be acceptable
- In cases of an exceptional circumstance (e.g. domestic emergency/acutely sick relative), staff must seek permission from a member of the Senior Management Team
- Staff should report any usage of mobile devices that causes them concern to the Headteacher

SOCIAL NETWORKING

Children's access to a range of social media is becoming part of their everyday Internet browsing e.g. Club Penguin accounts or Moshi Monsters, thus it is schools responsibility to raise awareness as to what is their personal information is and the implications of sharing this online.

Where are sites that have specific age restrictions children should be made aware of this. If a pupil has such accounts t**his is ultimately the parents' responsibly.** We feel that as part of Esafety lessons there should be an open discussion around such sites, where age restrictions and the implications of having such accounts are discussed. Schools should strive to raise awareness through parent meetings their responsibility when their children access such sites.

The element of how to set privacy settings MUST be included whenever discussing social media sites.

If there are concerns raised during these sessions the members of staff should go through the appropriate reporting procedure.

MAINTAINING THE SECURITY AND SAFETY OF THE SCHOOL NETWORK

We are aware that connection to the Internet significantly increases the risk that a computer or a computer network may be infected by a virus or accessed by unauthorised persons. As part of the ICT SLA agreement the school receives regular Anti-Virus software updates. However it is the schools duty to notify the LA if there is a possible virus risk.

Our internet access is purchased from BOLTON LA, and the school has a “fileserver” which acts as the schools server, this provides a service designed for pupils including a “firewall” filtering system intended to prevent access to material inappropriate for children;

Staff will check that the sites pre-selected for pupil use are appropriate to the age and maturity of pupils;

Staff will be particularly vigilant when pupils are undertaking their own search and will check that the children are following the agreed search plan;

Staff to ensure that when searching the Internet for images all projectors and Smartboards to be turned off or use the freeze tool enabling a wider use of images banks;

If staff or pupils discover unsuitable sites the COMPUTING co-ordinator will be informed. The URL (address) and content will be reported to the LA COMPUTING support team;

If it is thought that the material is illegal, after consultation with the LA ICT support team, the site will be referred to the Internet Watch Foundation and the police;

Our an AUP / Esafety Rules will be posted near computer systems;

The head teacher will ensure that the policy is implemented effectively.

REMOTE ACCESS

Where a teacher has access to school equipment out of school hours, teachers are encouraged to use these systems reasonably and appropriately.

All staff to be trained on how to save their files to the school network, home shared files and remote access. Removable media such as memory sticks, laptops, PDAs and mobile phones should not be used to store any sensitive or personal data.
Any data that could identify students or staff should not be removed from your school's network without necessary controls being in place. This includes emailing personal information to home PCs.

It is the experience of other schools that the above measures have been highly effective. However, due to the international scale and linked nature of information available via the Internet, it is not possible to guarantee that particular types of material will never appear on a computer screen. Neither the school nor BOLTON LA can accept liability for the material accessed, or any consequences thereof.

_____

I confirm that I have read and understood the E-Safety Policy and agree to abide by it.

Signed _____ Print _____ Date _____

Staff Acceptable Use Policy

Covers use of digital technologies in school: i.e. email, Internet, intranet and network resources, blog, software, equipment and systems.

- I will only use the school's digital technology resources and systems for Professional purposes or for uses deemed 'reasonable' by the Principal and Governing Body.
- I will not reveal my password(s) to anyone.
- I will not allow unauthorised individuals to access email / Internet / intranet / network, or other school / LA systems.
- I will ensure all documents, data etc., are saved, accessed and deleted in accordance with the school's network and data security and confidentiality protocols.
- I will not engage in any online activity that may compromise my professional responsibilities.
- I will only use the approved, secure email system(s) for any school business.
- I will only use the approved school email, school Learning Platform or other school approved communication systems with pupils or parents/carers, and only communicate with them on appropriate school business.
- I will not browse, download or send material that could be considered offensive to colleagues.
- I will report any accidental access to, or receipt of inappropriate materials, or filtering breach to the appropriate school E Safety Officer.
- I will not download any software or resources from the Internet that can compromise the network, or are not adequately licensed.
- I will not connect a computer, laptop or other device (including USB flash drive), to the network / Internet that does not have up-to-date anti-virus software, and I will keep any 'loaned' equipment up-to-date, using the school's recommended anti-virus, firewall and other COMPUTING 'defence' systems.
- I will not use personal digital cameras or camera phones for taking and transferring images of pupils or staff without permission and will not store images at home without permission.
- I will use the school's blog in accordance with school advice. (See Blogging Policy)

- I agree and accept that any computer or laptop loaned to me by the school, is provided solely to support my professional responsibilities and that I will notify the school of any "significant personal use" as defined by HM Revenue & Customs.
- I will ensure any confidential data that I wish to transport from one location to another is protected by encryption and that I follow school data security protocols when using any such data at any location.

- I understand that data protection policy requires that any information seen by me with regard to staff or pupil information, held within the school's information management system, will be kept private and confidential, EXCEPT when it is deemed necessary that I am required by law to disclose such information to an appropriate authority.

- I will embed the school's e-safety curriculum into my teaching. (See E-Safety Policy)

- Staff should NOT use their personal phones for school business or for taking photographs of children. Unless, in exceptional circumstances, an emergency telephone call needs to be made.

- Mobile phones should not be used when teaching, unless in an emergency.

Social Networks

The school recognises that many staff will actively use Facebook, Twitter, and other such social networking sites, blogging and messaging services. Staff must not post material (including text or images) which damages the reputation of the school or which causes concern about their suitability to work with children. Staff must recognise that it is not appropriate to discuss issues relating to children or other members of staff via these networks. Those who post material which could be considered as inappropriate could render themselves vulnerable to criticism or allegations of misconduct.

- It is never acceptable to accept a 'friendship request' from pupils at the school, as children attending The Ferns Primary Academy will be breaching terms and conditions of use of those sites age restriction policy. It is also inadvisable to accept as friends ex-pupils who are still minors. If a parent of a pupil seeks to establish contact, the member of staff should exercise their professional judgement at all times.

- It is advisable never to accept a 'friendship request' from a parent of 'The Ferns Primary Academy'.

- Setting a high security level on social networking sites as advisable. These sites regularly change the security settings, therefore staff should always strive to keep their profile in line with the securest settings.

- I will ensure that any private social networking sites / blogs etc that I create or actively contribute to are not confused with my professional role.

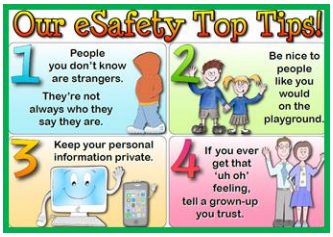
NOTE

It should be understood by all staff that this Code of Practice is in place to protect staff from potential risk in their use of COMPUTING / ICT in their everyday work.

The detail in this policy must be adhered to in its entirety. This has been developed with Northern Education Trust and is essential for the safeguarding of our children. Not following the policy will result in disciplinary action.

I confirm that I have read and understood the Acceptable Use Policy for Computing and agree to abide by it.

Signed _____ Print _____ Date _____



The Ferns Primary Academy

Years 1 and 2 Acceptable Use Agreement / eSafety Rules

	I will use school computers for school work and not to upset or be rude to other people. I will ask my teacher for help if I can't work the computer.
	I will look after the school's computers, laptops, camera's and tablets and tell a teacher straight away if something is broken or not working properly. I will log off or shut down a computer when I have finished using it.
108year20..	I will save only school work on the school network and will check with my teacher before printing. I will only open and close my own files.
	I will always use what I have learned about e-safety to keep myself safe and will tell a teacher if I get that 'uh oh' feeling. I will always for our 'SMART Rules'.
    	I will only use the internet with permission from my teacher. I will only go on websites that my teacher tells me to. I will tell my teacher straight away if I go on a website by mistake. I will tell a teacher straight away if I see a website that is not my work. I will only login to laptops and websites with my own username and password. I will only use words given to me when using a search engine. E.g. Google

Years 3 and 4 Acceptable Use Agreement / eSafety Rules

 	I will use school computers for school work and not to upset or be rude to other people but treat each other with respect. I will look after the school's computers, laptops, camera's and tablets and tell a teacher straight away if something is broken or not working properly. I will log off or shut down a computer when I have finished using it.
108year20..	I will save only school work on the school network and will check with my teacher before printing. I will only open and close my own files.
	I will always use what I have learned about e-safety to keep myself safe and will tell a teacher if I get worried or unhappy. I will always follow, use and talk about our 'SMART Rules'.
 The Ferns Academy Blog	I will only use my class email account / blog (which ends thefernsacademy.org) I will not open emails from people I don't know without checking with my teacher. I will only send messages/comments that are polite and friendly. I will not open any email attachments without checking with my teacher.
    	I will only use the internet with permission from my teacher. I will only go on websites that my teacher tells me to. I will tell a teacher straight away if I see a website that is not my work. I will only login to laptops and websites with my own username and password. When I use the internet to research a topic, I will try to use a detailed search and look for useful and reliable websites that will help me with my work.

Years 5 and 6 Acceptable Use
Agreement / eSafety Rules


I will use school computers for my school work and not to upset/be rude to other people or create a bad impression of my school.

I will make sure that my work does not break copyright (as discussed in lessons).

I will look after school ICT equipment and report any damage to a teacher straight away.

I will only use the usernames and passwords I have been given, and I will not tell other people.

I will only use **my** school blog username and password to help with my school work/homework, and will comment positively on other children's work.

I will only use my class email address when emailing to and from school.

I will not open any attachments without checking with an adult.


I will not deliberately search for, save or send anything that could be unpleasant or nasty. If I accidentally find anything like this I will tell my teacher immediately.

I will be responsible for my behaviour when using ICT because I know that these rules are to keep me safe.

I will shut down my computer when I am finished.

I know that my use of ICT can be checked and that my parent/carer contacted if a member of school staff is concerned about my eSafety.

I will always keep my personal details private (My name, family information, journey to school, my pets and hobbies are all examples of personal details).

I will not give my mobile phone number to anyone who is not a friend.

I will always check with a responsible adult before I show photographs of myself.

The Ferns Primary Academy

Dear Parent/ Carer

ICT (Soon to be replaced by 'Computing') including the internet, email and mobile technologies, etc has become an important part of learning in our school. We expect all children to be safe and responsible when using any ICT.

Please read and discuss these eSafety rules with your child and return the slip at the bottom of this page. If you have any concerns or would like some explanation please contact Mr Broadbent through the school office.

Our esafety policy as well as helpful websites and explanations can be found on our homepage on thefernsacademy.org website.

✂ -

Parent/ carer signature

We have discussed this and ………………………………………......(child name) agrees to follow the eSafety rules and to support the safe use of ICT / Computing at The Ferns Primary Academy.

Parent/ Carer Signature …………………….………………………….

Class ………………………………… Date ……………………………