Online Safety Policy

Agreed: Summer term 2023

Review: Summer term 2024

Contents

Introduction

The use of ICT in the 21st Century is seen as an essential resource to support learning and teaching, as well as playing an important role in the everyday lives of children, young people and adults. Consequently, schools need to build in the use of these technologies in order to arm our young people with the skills to access life-long learning and employment.
This has been even more relevant over recent years with children's use of remote learning and more exposure to the online world than ever before.

Information and Communications Technology covers a wide range of resources including; web-based and mobile learning. It is also important to recognise the constant and fast paced evolution of ICT within our society as a whole. Currently the internet technologies children and young people are using both inside and outside of the classroom include:

- Websites
- Learning Platforms (eg Google Classroom) and Virtual Learning Environments (VLE)
- Email and Instant Messaging
- Chat Rooms and Social Networking
- Blogs and Wikis
- Podcasting
- Video Broadcasting
- Music Downloading
- Gaming
- Mobile/ Smart phones with text, video and/ or web functionality

Whilst exciting and beneficial both in and out of the context of education, much ICT, particularly web-based resources, are not consistently policed. All users need to be aware of the range of risks associated with the use of these Internet technologies.

At Brigg Primary we know that many of our school have access to a range of device and the internet. We understand the responsibility to educate our pupils on online safety issues; teaching them the appropriate behaviours and critical thinking skills to enable them to remain both safe and legal when using the internet and related technologies, in and beyond the context of the classroom.

Responsibilities of the School Community

We believe that online is the responsibility of the whole school community, and everyone has their part to play in ensuring all members of the community are able to benefit from the opportunities that technology provides for learning and teaching.

The following responsibilities demonstrate how each member of the community will contribute.

Responsibilities of the Senior Leadership Team (including DSL)

- Develop and promote an Online safety culture within the school community.
- Support the Online safety coordinator in their work.
- Make appropriate resources, training and support available to members of the school community to ensure they are able to carry out their roles with regard to Online safety effectively.
- Receive and regularly review Online safety incident logs and be aware of the procedure to be followed should an Online safety incident occur in school.
- Take ultimate responsibility for the Online safety of the school community.

Responsibilities of the Computing Lead / IT support manager

- Promote an awareness and commitment to Online safety throughout the school.
- Be the first point of contact in school on all Online safety matters.
- Create and maintain Online safety policies and procedures.
- Develop an understanding of current Online safety issues, guidance and appropriate legislation.
- Ensure all members of staff receive an appropriate level of training in Online safety issues (Relevent training will be added to the 'Watch List' on National Collage.
- Ensure that Online safety education is embedded across the curriculum.
- Ensure that Online safety is promoted to parents and carers.
- Liaise with the local authority, the local safeguarding children's board and other relevant agencies as appropriate.
- Monitor and report on Online safety issues to the Online safety group and SLT as appropriate
- Ensure an Online safety incident log is kept up-to-date.

Ensure that school systems are secure and protected against virus and malware and that filtering is in place via Broadband provider (currently Schools Broadband)

Responsibilities of Teachers and Support Staff

- Read, understand and help promote the school's Online safety policies and guidance.
- Read, understand and adhere to the school staff Acceptable Use Policy (AUP).
- Develop and maintain an awareness of current Online safety issues and guidance.
- Model safe and responsible behaviours in your own use of technology.
- Embed Online safety messages in learning activities where appropriate.
- Supervise pupils carefully when engaged in learning activities involving technology.
- Be aware of what to do if an Online safety incident occurs and liaise with the DSLs.
- Maintain a professional level of conduct in their personal use of technology at all times.

Responsibilities of Pupils

- Read, understand and adhere to the school pupil AUP (contained in the home /school agreement booklet).
- Adhere to any policies and practices the school creates.
- Take responsibility for learning about the benefits and risks of using the Internet and other technologies in school and at home.
- Take responsibility for your own and each others' safe and responsible use of technology in school and at home, including judging the risks posed by the personal technology owned and used by pupils outside of school.
- Ensure you respect the feelings, rights, values and intellectual property of others in your use of technology in school and at home.
- Understand what action you should take if you feel worried, uncomfortable, vulnerable or at risk whilst using technology in school and at home, or if you know of someone who this is happening to.
- Discuss Online safety issues with family and friends in an open and honest way.

Responsibilities of Parents and Carers

- Help and support your school in promoting Online safety.
- Read, understand and promote the school pupil AUP with your children (contained in the home /school agreement booklet).
- Take responsibility for learning about the benefits and risks of using the Internet and other technologies that your children use in school and at home.
- take responsibility for their own awareness and learning in relation to the opportunities and risks posed by new and emerging technologies
- Discuss Online safety concerns with your children, show an interest in how they are using technology, and encourage them to behave safely and responsibly when using technology.
- Model safe and responsible behaviours in your own use of technology.
- Consult with the school if you have any concerns about your children's use of technology.

Parents can seek further guidance on keeping children safe online from the following organisations and websites:

- What are the issues? – UK Safer Internet Centre
- Hot topics – Childnet International
- Parent resource sheet – Childnet International
- Healthy relationships – Disrespect Nobody

Responsibilities of Governing Body

- Read, understand, contribute to and help promote the school's Online safety policies and guidance.
- Develop an overview of the benefits and risks of the Internet and common technologies used by pupils.
- Develop an overview of how the school ICT infrastructure provides safe access to the Internet.
- Develop an overview of how the school encourages pupils to adopt safe and responsible behaviours in their use of technology in and out of school.
- Support the work of the Online safety group in promoting and ensuring safe and responsible use of technology in and out of school, including encouraging parents to become engaged in Online safety activities.
- Ensure appropriate funding and resources are available for the school to implement their Online safety strategy.

Teaching and Learning

- We will provide a series of specific Online safety-related lessons in every year group/specific year groups as part of the computing curriculum / PSHE curriculum / other lessons.
- We will celebrate and promote Online safety through a planned programme of assemblies and whole-school activities, including promoting Safer Internet Day each year.
- We will discuss, remind or raise relevant Online safety messages with pupils routinely wherever suitable opportunities arise during all lessons; including the need to protect personal information, consider the consequences their actions may have on others, the need to check the accuracy and validity of information they use, and the need to respect and acknowledge ownership of digital materials. (Including relevant issues, such as 'sexting')
- We will remind pupils about their responsibilities through an AUP which every pupil will sign.
- Staff will model safe and responsible behaviour in their own use of technology during lessons.

Computing Curriculum

Pupils will be taught about online safety as part of both the computing curriculum and the PSHE/RHE curriculum:

In **Key Stage 1**, pupils will be taught to:

- Use technology safely and respectfully, keeping personal information private
- Identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies

Pupils in **Key Stage 2** will be taught to:

- Use technology safely, respectfully and responsibly
- Recognise acceptable and unacceptable behaviour

- Identify a range of ways to report concerns about content and contact

By the **end of primary school**, pupils will know:

- That people sometimes behave differently online, including by pretending to be someone they are not
- That the same principles apply to online relationships as to face-to-face relationships, including the importance of respect for others online including when we are anonymous
- The rules and principles for keeping safe online, how to recognise risks, harmful content and contact, and how to report them
- How to critically consider their online friendships and sources of information including awareness of the risks associated with people they have never met
- How information and data is shared and used online
- What sorts of boundaries are appropriate in friendships with peers and others (including in a digital context)
- How to respond safely and appropriately to adults they may encounter (in all contexts, including online) whom they do not know

How parents and carers will be involved

We believe it is important to help all our parents develop sufficient knowledge, skills and understanding to be able to help keep themselves and their children safe. To achieve this we will:

• include useful links and advice on Online safety regularly in newsletters / on our school website and promote
these via Class Dojo and our social media pages (Twitter and Facebook)

Cyber-bullying
Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of one person or group by another person or group, where the relationship involves an imbalance of power. (See also the school behaviour policy.)

Preventing and addressing cyber-bullying

To help prevent cyber-bullying, we will ensure that pupils understand what it is and what to do if they become aware of it happening to them or others. We will ensure that pupils know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.

The school will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Class teachers will discuss cyber-bullying with their classes

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes personal, social, health and economic (PSHE) education, and other subjects where appropriate.

All staff, governors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training.

The school also sends information/leaflets on cyber-bullying to parents so that they are aware of the signs, how to report it and how they can support children who may be affected.

In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school behaviour policy. Where illegal, inappropriate or harmful material has been spread among pupils, the school will use all reasonable endeavours to ensure the incident is contained.

The DSL will consider whether the incident should be reported to the police if it involves illegal material, and will work with external services if it is deemed necessary to do so.

Managing ICT Systems and Access

Current IT support contract: **South Farm CPA**

• The school will be responsible for ensuring that access to the ICT systems is as safe and secure as reasonably possible.
• Servers and other key hardware or infrastructure will be located securely with only appropriate staff permitted access.
• Servers, workstations and other hardware and software will be kept updated as appropriate.
• Virus protection is installed on all appropriate hardware, and will be kept active and up-to-date (Sophos)
• The school will agree which users should and should not have internet access, and the appropriate level of access and supervision they should receive.
• All users (Staff/Pupils/Volunteers/Parent Helpers) will sign an end-user Acceptable Use Policy (AUP) provided by the school, appropriate to their age and access. Users will be made aware that they must take responsibility for their use of, and behaviour whilst using, the school ICT systems, and that such activity will be monitored and checked.
• Pupils will access the internet on laptops using a class log-on, which the teacher supervises. All Internet access will be by working alongside a member of staff, or if working independently a member of staff will supervise at all times.
• Use of the internet on tablets (iPads) will be monitored via a management system.
• When using Chromebooks, children will log on using their own @briggprimary.co.uk account. Internet use and app access is centrally managed by the administrator.
• Members of staff will access the Internet using an individual log-on, which they will keep secure. They will ensure they log-out after each session, and not allow pupils to access the Internet through their log-on. Staff tablets (iPads) should be only used by pupils under supervision.
• They will abide by the school AUP at all times.

• Any administrator or master passwords for school ICT systems should be kept secure and available to at least two members of staff, e.g. head teacher and Computing curriculum leader as well as **South Farm CPA**.
• The school will take all reasonable precautions to ensure that users do not access inappropriate material. However, it is not possible to guarantee that access to unsuitable material will never occur.
• The school will regularly audit ICT use to establish if the Online safety policy is adequate and that the implementation of the Online safety policy is appropriate. The school will regularly review our Internet access provision, and review new methods to identify, assess and minimise risks.

Filtering Internet access

• The school uses a filtered Internet service. The filtering is provided via Schools Broadband (netsweeper) provision. Access to filtering service also given to **South Farm CPA**.
• If users discover a website with inappropriate content, this should be reported to a member of staff who will inform the Online safety coordinator
• If users discover a website with potentially illegal content, this should be reported immediately to the Online safety coordinator. The school will report this to the LA. Any potential breaches discovered wil be fully investigated, challenged and reported as necessary.
• The school will regularly review the filtering and other security systems to ensure they meet the needs of all users. Staff and pupils use different ports when accessing the internet to reflect the different filtering parameters.

Learning technologies in school

School staff have the specific power under the Education and Inspections Act 2006 (which has been increased by the Education Act 2011) to search for and, if necessary, delete inappropriate images or files on pupils' electronic devices, including mobile phones, iPads and other tablet devices, where they believe there is a 'good reason' to do so.

When deciding whether there is a good reason to examine or erase data or files on an electronic device, staff must reasonably suspect that the data or file in question has been, or could be, used to:

- Cause harm, and/or
- Disrupt teaching, and/or
- Break any of the school rules

If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL or other member of the senior leadership team to decide whether they should:

- Delete that material, or

- Retain it as evidence (of a criminal offence or a breach of school discipline), and/or
- Report it to the police*

* Staff may also confiscate devices for evidence to hand to the police, if a pupil discloses that they are being abused and that this abuse includes an online element.

Any searching of pupils will be carried out in line with:

- The DfE's latest guidance on screening, searching and confiscation
- UKCIS guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people

Any complaints about searching for or deleting inappropriate images or files on pupils' electronic devices will be dealt with through the school complaints procedure.

	Pupils	**Staff**
Personal mobile phones brought into school	Allowed with permission and stored by staff during school day	Allowed
Mobile phones used during lessons	Not allowed	For photography purposes only
Mobiles phones used outside lessons	Not allowed	Allowed
School mobile on trips	Not allowed	Allowed
Taking photographs / video on personal equipment	Not allowed	Allowed *photos to be backed up to school google photo account / laptop and removed from device as soon as possible.
Taking photographs / video on school devices	Allowed with permission * any images published with parents permission (annual consent form)	Allowed * any images published with parents permission (annual consent form)
Use of hand held devices, such as PDAs, MP3 players or personal gaming consoles	Allowed with permission *School equipment only	Allowed
Use of personal email addresses in school	Not allowed	Allowed (outside teaching hours)
Use of school email	Allowed with	Allowed (via school domain gmail account

addresses	permission (via school domain gmail account)	or @northlincs account)
Use of online chat rooms	Not allowed	Not allowed
Use of instant messaging services	Not allowed except as part of a planned teacher led activity	Not allowed except as part of a planned teacher led activity
Use of blog, wikis, podcasts or social networking sites	Allowed with supervision	Allowed *Only school accounts, eg Class Dojo, Twitter
Use of video conferencing	Allowed with permission (Google Meet)	Allowed with permission (Google Meet internal / others from outside agencies links)

Using email

• Staff and pupils should use approved e-mail accounts allocated to them by the school (@briggprimary.co.uk), and be aware that their use of the school e-mail system may be monitored and checked.
• Pupils may be allocated e-mail accounts/addresses for their use in school under supervision of the class teacher. Classes may be allocated (@briggprimary.co.uk) email address as required, linked to curriculum coverage in enable local, national or global links.
• Pupils will be reminded when using e-mail about the need to send polite and responsible messages, about the dangers of revealing personal information, about the dangers of opening e-mail from an unknown sender, or viewing/opening attachments.
• Staff and pupils are not permitted to access personal e-mail accounts (on staff machines) during school hours
• Communication between staff and pupils or members of the wider school community should be professional and related to school matters only.
• Any inappropriate use of the school VLP or e-mail system, or the receipt of any inappropriate messages by a user, should be reported to a member of staff immediately.

Using images, video and sound

The school will remind pupils of safe and responsible behaviours when creating, using and storing digital images, video and sound. We will remind them of the risks of inappropriate use of digital images, video and sound in their online activities both at school and at home.

Digital images, video and sound will only be created using equipment provided by the school and for school related activities.
• In particular, digital images, video and sound will not be taken without the permission (as per annual consent forms) of participants; images and video will be of appropriate activities and participants will be in appropriate dress; full names of participants will not be used

either within the resource itself, within the file-name or in accompanying text online; such resources will not be published online without the permission of the staff/pupils involved.
• If pupils are involved, relevant parental permission will also be sought before resources are published online (Home/School agreement booklet).

Using blogs, wikis, podcasts, social networking and other ways for pupils to publish content online

• Any public blogs run by staff on behalf of the school will be hosted on the learning platform/school website and will be monitored by the Online Safety Lead. School Twitter accounts and Facebook pages will be managed by the members of the SLT and managed access may be provided to other members of staff.
• Pupils will model safe and responsible behaviour in their creation and publishing of online content within the school learning platform. For example, pupils will be reminded not to reveal personal information which may allow someone to identify and locate them. Pupils will not use their real name when creating such resources. They will be encouraged to create an appropriate 'nickname'.
• Staff and pupils will be encouraged to adopt similar safe and responsible behaviours in their personal use of blogs, wikis, social networking sites and other online publishing outside of school.

Using mobile phones

• Staff phones should be turned off or on silent and be stored away from pupils. Calls should be made / received in private, during non-contact time.
• KS2 Pupils can bring mobile phones to school, but must be handed in to a member of staff, who will store the securely until home time.
• Where staff members are required to make phone call for school duties, for instance in case of emergency during off-site activities, or for contacting pupils or parents, staff will not be expected to use their personal mobile phones in any situation (where their mobile phone number or other personal details may be revealed to a pupil or parent.)
Staff should contact the school office, who will then contact the relevant people.
(See Emergency Plan for additional information regarding use of personal mobiles)

Mobile phones are a common vehicle for cyberbullying, through the recording of inappropriate images or video, distributing such images and videos via Bluetooth or other wireless technologies, or the sending of abusive text messages. The school has referred to cyber bullying in the Anti-Bullying policy.

Using new technologies

• As a school we will keep abreast of new technologies and consider both the benefits for teaching and learning and also the risks from an Online safety point of view.
• The school will regularly amend the Online safety policy to reflect any new technology that we use, or to reflect the use of new technology by pupils which may cause an Online safety risk.

.

Protecting personal data

• The school will ensure personal data is recorded, processed, transferred and made available according to the Data Protection Act 2018 (Business Manager main contact).
• Staff will ensure they properly log-off from a computer terminal after accessing personal data. During inactivity devices should be 'locked'

- Passwords should be secure (8 characters long, combination of upper/lowercase letters/numbers.
- External hard drives should be encrypted.
- School laptops and devices should not be shared with friends or friends.

• Staff will not remove personal or sensitive data from the school premises without ensuring such data is kept secure, using encrypted devices only. Passwords for cloud services (eg Scholar Pack / Otrack)
• School iPads must be set up with the school staff passcode to ensure data protection.

The school website and other online content published by the school

• The school website/app will not include the personal details, including individual e-mail addresses or full names, of pupils.
• A generic contact form will be used for all enquiries received through the school website which will forward messages to the office.
• Individual staff email addresses may be published on the class pages/school app
• All content included on the school website, school app and social media posts will be checked by the SLT.
• The content of the website will be composed in such a way that individual pupils cannot be clearly identified.
• Staff and pupils should not post school-related content on any external website without seeking permission first.

Dealing with Online safety incidents

Guidance: What to do if? (taken from LSCB guidance)

An inappropriate website is accessed unintentionally by a child, young person or member of staff.

1. Play the situation down; don't make it into a drama.
2. Report to the head teacher/child protection coordinator and decide whether to inform parents of any children who viewed the site.
3. Inform the school technicians and ensure the site is filtered
4. Inform the LA if the filtering service is provided via an LA/RBC.

An inappropriate website is accessed intentionally by a child.

1. Refer to the acceptable use policy that was signed by the child, and apply agreed sanctions.
2. Notify the parents of the child.
3. Inform the school technicians and ensure the site is filtered if need be.
4. Inform the LA if the filtering service is provided via an LA/RBC.

An adult uses School IT equipment inappropriately.

1. Ensure you have a colleague with you, do not view the misuse alone.
2. Report the misuse immediately to the head teacher and ensure that there is no further access to the PC or laptop.
3. If the material is offensive but not illegal, the head teacher should then:
    - Remove the PC to a secure place.
    - Instigate an audit of all ICT equipment by the school's ICT managed service providers to ensure there is no risk of pupils accessing inappropriate materials in the school.
    - Identify the precise details of the material.
    - Take appropriate disciplinary action (contact Personnel/Human Resources).
    - Refer the incidence to the Local Authority Designated Officer (LADO)
    - Inform governors of the incident.
4. In an extreme case where the material is of an illegal nature:
    - Contact the local police or High Tech Crime Unit and follow their advice.
    - If requested remove the PC to a secure place and document what you have done.

A bullying incident directed at a child occurs through email or mobile phone technology, either inside or outside of school time.

1. Advise the child not to respond to the message.
2. Refer to relevant LSCB policies and procedures including what to do if you are worried, Online safety anti-bullying and PHSE and apply appropriate sanctions.
3. Secure and preserve any evidence.
4. Inform the sender's e-mail service provider.
5. Notify parents of the children involved.

6. Consider delivering a parent workshop for the school community.
7. Inform the police if necessary.
8. Inform the LA Online safety officer.

Malicious or threatening comments are posted on an Internet site about a pupil or member of staff.

1. Inform and request the comments be removed if the site is administered externally.
2. Secure and preserve any evidence.
3. Send all the evidence to CEOP at ww.ceop.gov.uk/contact_us.html.
4. Endeavour to trace the origin and inform police as appropriate.
5. Inform LA Online safety officer.

The school may wish to consider delivering a parent workshop for the school community

You are concerned that a child's safety is at risk because you suspect someone is using communication technologies (such as social networking sites) to make inappropriate contact with the child

1. Report to and discuss with the named child protection officer in school and contact parents.
2. Advise the child on how to terminate the communication and save all evidence.
3. Contact CEOP http://www.ceop.gov.uk/
4. Consider the involvement of the police and social services.
5. Inform LA Online safety officer who is The Head of Safeguarding and Practice
6. Consider delivering a parent workshop for the school community.

All of the above incidences must be reported immediately to the head teacher and Online safety officer.

Children should be confident in a no-blame culture when it comes to reporting inappropriate incidents involving the internet or mobile technology: they must be able to do this without fear.

Useful Websites

http://www.northlincslscb.co.uk/

www.thinkuknow.co.uk

www.kidsmart.org.uk

https://www.nspcc.org.uk/preventing-abuse/keeping-children-safe/onlinOnline safety/

www.childnet.com

www.safetynetkids.org.uk/personal-safety/staying-safe-online

www.bbc.co.uk/cbbc/shows/stay-safe

https://www.saferinternet.org.uk/

1.

Acceptable Use Policy - Staff

This policy covers the use of digital technologies in school: i.e email, internet, intranet and network resources, learning platform, software, mobile technologies, systems 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 Head and Governing Body.
- I will only use the school approved, secure email system(s) for any school business i.e. @briggprimary.co.uk and @northlincs.gov.uk email.
- I will not browse, download or send material that could be considered offensive to colleagues and any other individuals.
- I will report any accidental access to, or receipt of inappropriate materials, or filtering breach to the appropriate line manager/school named contact: Mrs Winter.
- I will not allow unauthorised individuals to access email/internet/intranet/network, or other school/LA systems.
- I will ensure that all my secure login credentials (including passwords) are not shared with any other individuals, displayed or used by any individual other than myself.
- I will not download any software, apps or resources from the internet that can compromise the network, or are not adequately licensed.
- I will follow the guidance in the People who work with Young People document and ensure that my personal email accounts, mobile/home telephone numbers are not shared with children, young people or families.
- I understand that all internet usage/and network usage can be logged and this information could be made available to my manager upon request.
- I will ensure that all documents are labelled, saved, accessed and deleted in accordance with the school's network security and confidentiality protocols, which ensure minimum mandatory compliance with the Cabinet Officer Data handling Procedures in Government : www.cabinetoffice.gov.uk/reports/data_handling.aspx
- I will not connect a computer, laptop or other device, to the network/internet that has not been approved by the school and meets its minimum security specification (i.e. up to date approved Anti virus etc.)
- 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.
- I will not engage in any online activity that may compromise my professional role this includes any comments made on personal social media messaging platforms.
- I agree and accept that any computer / laptop / mobile device loaned to me by the school is provided solely to support my professional responsibilities and that I will

notify the school of any software, apps or device relating to personal use to ensure that it does not breach the school policies.

- I will ensure any confidential information that I wish to transport from one location to another is protected by encryption, using the school USB drives.
- Mobile phones, mobile devices and the internet should not be accessed on site in a personal capacity with children present
- I understand that data protection policy requires that any information seen by me with regard to staff or pupil information, held within any schools system (e.g. MIS, Learning Platforms etc), 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 ensure I am aware of digital safeguarding issues so that they are appropriately embedded in my classroom practice.
- I will only use LA systems in accordance with any corporate policies.
- I understand that failure to comply with the Acceptable Use Policy could lead to disciplinary action.

User Signature

- I understand that it is my responsibility to ensure that I remain up to date and read and understand the schools most recent Acceptable Use Policy (normally an annual revisit).
- I agree to abide by the schools most recent Acceptable Use Policy.
- I wish to have an email account; be connected to the intranet and internet; be able to use the schools ICT resources and systems.
- I understand that all my activity and usage of the school ICT system can be monitored and information on such activity and usage can be accessed and actioned upon to safeguard myself and others.

Signature………

Date………

Full Name……….

Job Title…………………………………………………………………………………………….………………

School………..…

Professionals' Online safety Agreement
Inc Students, Parent Helpers and Volunteers

- In line with the school's Safeguarding and Online safety policies any visitors to school need to agree to the following statements.

- I will not use my personal mobile phone or similar devices whilst in the presence of children or within the school building between the hours of 8.45am and 3.45pm. The school's telephone number can be given as a point of contact if out of the school building.

- I will not use personal digital cameras or camera phones.

- I will ensure that any private social networking sites / blogs etc that I create or actively contribute to will not contain any information regarding school activities, children or their behaviour.

- I will notify staff immediately if I hear or see anything of a confidential nature and any information will not be discussed outside of school. I will not discuss any children or their behaviour, with anyone outside of school.

Signature ____

Date ____

Full Name ____