Ponteland Community Primary School

E Safety Policy 2020/21 to include KS3

Policy approved by Head Teacher: _____ Date: 20 February 2020

Policy approved by Governing Body: _____ Date:
(Chair of Trustees)

Trustees to sign page 6 and 17
Staff to sign page 18

What Is E-Safety?

In today's society, children, young people and adults interact with technologies such as mobile phones, games consoles and the Internet on a daily basis and experience a wide range of opportunities, attitudes and situations. The exchange of ideas, social interaction and learning opportunities involved are greatly beneficial to all, but can occasionally place children, young people and adults in danger.

E-Safety covers issues relating to children and young people as well as adults and their safe use of the Internet, mobile phones and other electronic communications technologies, both in and out of school. It includes education for all members of the school community on risks and responsibilities and is part of the 'duty of care' which applies to everyone working with children.

●The school has appointed an e–Safety Coordinator.
●The e–Safety Policy and its implementation will be reviewed regularly.
●Our e–Safety Policy has been written by the school, building on e–Safety Policy and government guidance.
●Our School Policy has been agreed by the Senior Leadership Team and approved by trustees and other stakeholders such as the Parents' Forum.
●The School has appointed a member of the Governing Body to take lead responsibility for e-Safety

The School e-Safety Coordinator is Dr Pryer

Why Is E-Safety Important?

Teaching and Learning
Activities involving the internet and communications technologies might have been a rarity a few years ago, they are now common place. Coupled with this, pupils have access to these technologies outside of school and potentially through a range of locations; home, libraries, free wifi sites and also through a variety of technologies ranging from mobile phones to portable games machines.

The use of technology also brings many learning benefits and so risks need to be balanced up with the opportunities technology offers, and moderated by the careful and rigorous application of safety measures by schools. All users, be they children or adults are given a clear understanding of what the risks and dangers are, and how these can be safely managed.

Becta in 'Safeguarding Children in a Digital World' comment:
'While it is clear that technology offers children unprecedented opportunities to learn, communicate, create, discover and be entertained in a virtual environment, there are some inherent risks. And whilst most children's confidence and competence in using the technologies is high, their knowledge and understanding of the risks may be low.'

It is this challenge we need to tackle at Ponteland Community Primary School. Our aim is to ensure that pupils are not just safe in school, but are prepared for the outside world and the use of these technologies in the home and community.

Why Is Internet Use Important?

The rapid developments in electronic communications are having many effects on society.

- Internet use is part of the statutory curriculum and is a necessary tool for learning.
- The Internet is a part of everyday life for education, business and social interaction.
- The school has a duty to provide students with quality Internet access as part of their learning experience.
- Pupils use the Internet widely outside school and need to learn how to evaluate Internet information and to take care of their own safety and security.
- The purpose of Internet use in school is to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the school's management functions.
- Internet access is an entitlement for students who show a responsible and mature approach to its use.

How Does Internet Use Benefit Education?

A number of studies and government projects have identified the educational benefits to be gained through the appropriate use of the Internet including increased pupil attainment.
Benefits of using the Internet in education include:
●access to worldwide educational resources including museums and art galleries;
●inclusion in the National Education Network which connects all UK schools;
●educational and cultural exchanges between pupils worldwide;
●vocational, social and leisure use in libraries, clubs and at home;
●access to experts in many fields for pupils and staff;
●professional development for staff through access to national developments, educational materials and effective curriculum practice;
●collaboration across networks of schools, support services and professional associations;
●improved access to technical support including remote management of networks and automatic system updates;
●exchange of curriculum and administration data with Northumberland County Council and DfE;
●access to learning wherever and whenever convenient.

How Can Internet Use Enhance Learning?

●The school's Internet access is designed to enhance and extend education.
●Pupils are taught what Internet use is acceptable and what is not and given clear objectives for Internet use.
●The school ensures that the copying and subsequent use of Internet-derived materials by staff and pupils complies with copyright law.
●Access levels to the internet is reviewed to reflect the curriculum requirements and the age and ability of pupils.
●Staff should guide pupils to online activities that will support the learning outcomes planned for the pupils' age and ability.
●Pupils are educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.
●Pupils are taught to acknowledge the source of information used and to respect copyright when using Internet material in their own work.

How Will Pupils Learn How To Evaluate Internet Content?

●Pupils are taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
●Pupils use age-appropriate tools to research Internet content.
●The evaluation of online materials is a part of teaching and learning in every subject and is viewed as a whole-school requirement across the curriculum.

How Will Cyberbullying Be Managed?
Cyberbullying can be defined as "The use of Information Communication Technology, particularly mobile phones and the internet to deliberately hurt or upset someone" DCSF 2007.
Many young people and adults find that using the internet and mobile phones is a positive and creative part of their everyday life. Unfortunately, technologies can also be used negatively. When children are the target of bullying via mobiles phones, gaming or the Internet, they can often feel very alone, particularly if the adults around them do not understand cyberbullying and its effects. A once previously safe and enjoyable environment or activity can become threatening, harmful and a source of anxiety.
At Ponteland Community Primary School, pupils are taught what cyberbullying means and how to report it. DfE and Childnet resources and guidance are used to give pupils practical advice and guidance on cyberbullying: http://www.digizen.org/cyberbullying. These resources are used in ICT and PSHE and Citizenship lessons.

- Cyberbullying (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.
- There are clear procedures in place to support anyone in the school community affected by cyberbullying.

1. Roles and Responsibilities
The following section outlines the roles and responsibilities for e-safety of individuals and groups within the school:

Trustees:
Trustees are responsible for the approval of the E-Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the trustees receiving termly updates about e-safety incidents and monitoring reports. A member of the Governing Body has delegated the role of E-Safety Trustee to the Headteacher.

The role of the E-Safety trustee will include:
• termly meetings with the E-Safety Co-ordinator
• termly monitoring of e-safety incident logs
• reporting incidents to the Curriculum Committee

See section 2 Trustees E Safety Checklist

Headteacher and Senior Leaders:
• The Headteacher is responsible for ensuring the safety (including e-safety) of members of the school community.
• The Headteacher is responsible for ensuring that all relevant staff receive suitable CPD to enable them to carry out their e-safety roles and to train other colleagues, as relevant.
• The Headteacher will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal e-safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles. The Senior Leadership Team will receive regular monitoring reports.
• The Headteacher and another member of staff should be aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff (See section 7 for a flow chart on dealing with e-safety incidents "Reporting an E-Safety incident" and relevant Local Authority HR / disciplinary procedures).

E-Safety Coordinator (Dr Pryer)
The e-safety coordinator is responsible for:
• reporting incidents of misuse to the appropriate member of staff
• taking day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policies / documents
• ensuring that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place.
• providing training and advice for staff
• liaising with the Local Authority
• keeping log of incidents to inform future e-safety developments
• meeting regularly with E-Safety trustees to discuss current issues, review incident logs and filtering / change control logs
• attending relevant meetings
•discussing regularly to Senior Leadership Team

Network Manager / Technical staff:
The above people are responsible for ensuring:
• that the school's ICT infrastructure is secure and is not open to misuse or malicious attack
• that the school meets the e-safety technical requirements outlined in any relevant Local Authority E-Safety Policy and guidance
• that users may only access the school's network on protected machines
• that he/she keeps up to date with e-safety technical information in order to effectively carry out their e-safety role and inform others as relevant
• that the use of the network/ remote access/email is regularly monitored in order that any misuse / attempted misuse can be reported to the E-Safety Co-ordinator for investigation/ sanction/ action
• that monitoring software systems are implemented and updated as agreed in school policies.

Teaching and Support Staff:
are responsible for ensuring that:
• they have an up to date awareness of e-safety matters and of the current school safety policy and practices
• they have read, understood and signed the school Staff Acceptable Use Policy / Agreement (AUP)
• they report any suspected misuse or problem to the E-Safety Co-ordinator and ICT Co-ordinator for investigation / action / sanction
• digital communications with students / pupils (email / Virtual Learning Environment) should be on a professional level and only carried out using official school systems
• e-safety issues are embedded in all aspects of the curriculum and other school activities
• pupils understand and follow the school e-safety and acceptable use policy
• pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
• they monitor ICT activity in lessons, extra curricular and extended school activities
• they are aware of e-safety issues related to the use of mobile phones, cameras and hand held devices and that they monitor their use and implement current school policies with regard to these devices
• in lessons where internet use is pre-planned students / pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches

Designated Child Protection Officer:
should be trained in e-safety issues and be aware of the potential for serious child protection issues to arise from:
• sharing of personal data
• access to illegal / inappropriate materials
• inappropriate on-line contact with adults / strangers
• potential or actual incidents of grooming
• cyber-bullying

Pupils:
• are responsible for using the school ICT systems in accordance with the Pupil Acceptable Use Policy, which they will be expected to sign before being given access to school systems.
• have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
• need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
• will be expected to know and understand school policies on the use of mobile phones, digital cameras and hand held devices. They should also know and understand school policies on the taking / use of images and on cyber-bullying.
• should understand the importance of adopting good e-safety practice when using digital technologies out of school and realise that the school's E-Safety Policy covers their actions out of school, if related to their membership of the school

Parents / Carers:
Parents / Carers play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way. Research shows that many parents and carers do not fully understand the issues and are less experienced in the use of ICT than their children. The school will therefore take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website / VLE and information about national / local e-safety campaigns / literature.

Parents and carers will be responsible for:
• endorsing (by signature) the Student / Pupil Acceptable Use Policy
• accessing the school website / on-line pupil records in accordance with the relevant school Acceptable Use Policy.

Community Users, Volunteers and Supply Staff:
Users who access school ICT systems / website / VLE as part of the Extended School provision, as a volunteer or supply staff will be expected to sign the Staff, Volunteer and Third Party User AUP, before being provided with access to school systems.

2. Trustees E-Safety Checklist

Action	Completed by:
The Acceptable Use Policy is in place and has been revised to accommodate any developments in technology and its use.	Caroline Pryer 10.03.20
Trustees know that all staff (teaching and non-teaching) and any volunteers or supply staff are familiar with the current e-safety policy and the Acceptable Use Policy.	Caroline Pryer 10.03.20
e-Safety forms part of the induction of all new staff	Emma Clayton / Caroline Pryer 10.03.20
Trustees know that all new parents/carers have received a copy of the school's AUP.	Emma Clayton 10.03.20
Trustees know that all parents/ carers have signed a copy of the internet access permission form in the child's diary.	Caroline Pryer 10.03.20
All staff (teaching and non-teaching) and any volunteers or supply staff are in possession of the 'A concern is raised' flow diagram and know what to do if an incident occurs.	Emma Clayton / Caroline Pryer 10.03.20
All users are compliant with additional AUP and Terms and conditions contained in other services and procedures are in place to ensure this happens.	Caroline Pryer 10.03.20
All users understand the use of e-safety monitoring software where installed.	Caroline Pryer 10.03.20

Chair of Governing Body:

_____ Date:

(Signature)

3. Unsuitable / Inappropriate / Illegal activities

The school believes that the activities referred to in the following section would be inappropriate in a school context and those users, as defined below, should not engage in these activities in school or outside school when using school equipment or systems. The school policy restricts certain internet usage as follows:

	Acceptable	Acceptable at times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
child sexual abuse images					**X**
promotion or conduct of illegal acts, e.g. under child protection, obscenity, computer misuse and fraud legislation					**X**
adult material that potentially breaches the Obscene Publications Act in the UK					**X**
criminally racist material in UK					**X**
pornography				**X**	
promotion of any kind of discrimination				**X**	
promotion of racial or religious hatred				**X**	
threatening behaviour, including promotion of physical violence or mental harm				**X**	
any other information which may be offensive to colleagues, breaches the integrity of the ethos of the school or brings the school into disrepute				**X**	
Using school systems to run a private business				**X**	
Use systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by Northumberland LA and /or Ponteland Community Primary School				**X**	
	Acceptable	**Acceptable at times**	**Acceptable for nominated users**	**Unacceptable**	**Unacceptable and illegal**
Uploading, downloading or transmitting commercial software or any copyrighted materials				**X**	

belonging to third parties, without the necessary licensing permissions					
Revealing or publicising confidential or proprietary information (e.g. financial / personal, databases, computer / network access codes and passwords)				**X**	
Creating or propagating computer viruses or other harmful files				**X**	
Carrying out sustained or instantaneous high volume network traffic (downloading / uploading files) that causes network congestion and hinders others in their use of the internet				**X**	
On-line gaming (educational)		**X**			
On-line gaming (non educational)				**X**	
On-line gambling				**X**	
On-line shopping / commerce			**X**		
File sharing				**X**	
Use of social networking sites apart from Merlin e.g. Bebo, Facebook for older users			**X**		
Use of video broadcasting e.g. Youtube			**X (Staff)**		

4. Communications

A wide range of rapidly developing communications technologies has the potential to enhance learning. The following table shows how the school currently considers the benefit of using these technologies for education outweighs their risks / disadvantages:

	Staff & other adults				**Pupils**			
Communication Technologies	**Allowed**	**Allowed at certain times**	**Allowed with permission**	**Not allowed**	**Allowed**	**Allowed at certain times**	**Allowed with staff permission**	**Not allowed**
Mobile phones may be brought to school	**X**							**X**
Use of mobile phones in lessons				**X**				**X**
Use of mobile phones in social time	**X**							**X**
Taking photographs on camera devices			**X**					**X**

Taking photographs on personal mobile phones				**X**				**X**
Use of hand held devices e.g. iPads in lessons			**X**				**X**	
Use of personal email address in school, or on school network			**X**					**X**
Use of school email for personal emails			**X**					**X**
Use of chat rooms / facilities for personal use				**X**				**X**
Use of instant messaging for personal use				**X**				**X**
Use of social networking sites for personal use				**X**				**X**
Use of blogs			**X**					**X**

5. Responding to incidents of misuse

It is hoped that all members of the school community will be responsible users of ICT, who understand and follow this policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse. Listed below are the responses that will be made to any apparent or actual incidents of misuse:

If apparent or actual misuse appears to involve illegal activity i.e;

- child sexual abuse images
- adult material which potentially breaches the Obscene Publications Act
- criminally racist material
- other criminal conduct, activity or materials

The flow chart issued by the Northumberland Safeguarding Children Board must be consulted and actions followed in line with the flow chart, in particular the sections on reporting the incident to the police and the preservation of evidence. This flowchart indicating how to proceed can be found at the back of this policy. All members of staff have received training about this matter and have been issued with a copy of the flowchart.

If members of staff suspect that misuse might have taken place, but that misuse is not illegal, it is essential that correct procedures are used to investigate, preserve evidence and protect those carrying out the investigation. At Ponteland Community Primary School, like other schools in Northumberland, when an incident occurs it is important that we keeps a clear record of what has and is taking place. At PCPS we will use the recording log.

It is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the school community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal behaviour / disciplinary procedures as follows:
The Curriculum Network and Internet Usage will be monitored through PCE and reports will be provided weekly and as requested. Any incident or deliberate misuse will be reported immediately to either the

Designated Child Protection Officers, Dr Pryer and Mrs Cafferty (in the case of pupil misuse), or to the Head teacher (in the case of staff or volunteer misuse).

Incidents of pupil misuse will be addressed by the school pupil disciplinary systems and reported to the Trustees Curriculum Committee. Incidents of Staff/ Volunteer misuse will be addressed using the Staff Disciplinary Procedures and reported to the Chair of Trustees.

Policy Central Enterprise (PCE)

As part of our duty of care, we have a legal obligation to closely monitor access to their network and the Internet. At Ponteland Community Primary School we use the County Council approved system to monitor, report and alert facilities of potential computer misuse as part of our e-Safety strategy. This software monitors all pupil and staff devices in the school and offers a wide range of features to ensure the online safety of pupils and staff, in particular identifying and preventing:

•Bullying and threatening behaviour
•Abusive comments or offensive attitudes
•Inadvertent exposure to inappropriate web sites (pornography, violence, suicide)
•Deliberate access to inappropriate web sites
•Online gambling and shopping
•Un-moderated discussion forums and chat rooms.

6. Responding to Incidents Reporting Log

Northumberland County Council

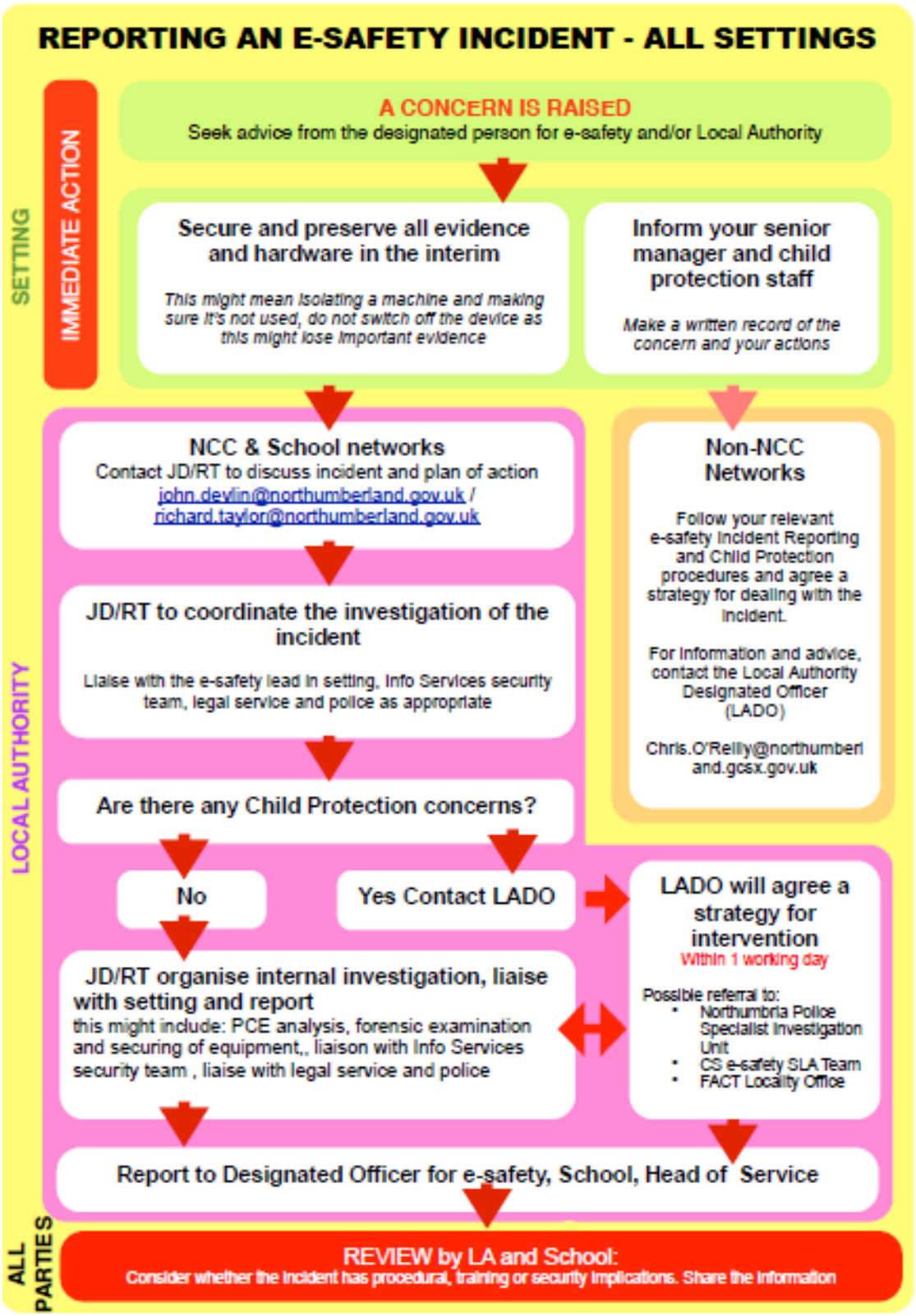
e-safety Incident Report

Name of school: _____

This Event Report Form Compiled By: Name Title Date	
Staff informed: Name & Date Headteacher e-safety co-ordinator Child protection officer Other	
Nature of Concern: Who was involved: pupil/staff/parents?	
Where did it occur: home, school?	
Time and date of Incident:	
Time and date the incident was logged:	
Action taken: (please tick)	

Evidence preserved Senior staff informed Other action	
Incident witnessed by: Staff Pupil Parent Other	
Other Officers Involved in Response: LA Officer LADO NCC Network Security Manager Other	
Follow up Action:	
Evidence Collected (and where retained):	
Review Date if required:	

7. Reporting an E-Safety incident (flow chart)



8. Actions and Sanctions for Pupils and Staff

Pupils **Actions/ Sanctions**

Incidents:	Refer to class		Refer to Headteacher	Refer to Police	Refer to technical support staff for action	Inform	Removal of network/ internet access rights	Warning	Further sanction e.g. detention/ exclusion
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).			X	X		X	X	X	X
Unauthorised use of non-educational sites during lessons	X		X			X			
Unauthorised use of mobile phone/ digital camera/ other handheld device	X		X			X			
Unauthorised use of social networking/ instant messaging/ personal e-mail	X		X			X			
Unauthorised downloading or uploading of files	X		X			X			
Allowing others to access school network by sharing username and passwords	X		X			X			
Attempting to access or accessing the school network, using another pupil's account	X		X		X	X			
Attempting to access or accessing the school network, using the account of a member of staff			X		X	X			
Corrupting or destroying the data of other users			X		X	X			
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature			X			X			
Continued infringements of the above, following previous warnings or sanctions			X			X	X	X	X
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school			X						
Using proxy sites or other means to subvert the school's filtering system			X		X	X	X	X	X
Accidentally accessing offensive or pornographic material and failing to report the incident			X		X	X	X	X	
Deliberately accessing or trying to access offensive or pornographic material			X			X	X	X	X
Receipt of transmission of material that infringes the copyright of another person or infringes the Data Protection Act			X			X			

Staff **Actions/ Sanctions**

Incidents:		Refer to Headteacher	Refer to Local Authority	Refer to Police	Refer to technical support staff for action	Warning	Suspension	Disciplinary action
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).		X	X	X		X	X	X
Excessive or inappropriate personal use of the internet / social networking sites/ instant messaging / personal email		X						
Unauthorised downloading or uploading of files		X			X	X		
Allowing others to access school network by sharing username and passwords or attempting to access or accessing the school network, using another person's account		X			X	X		
Careless use of personal data eg holding or transferring data in an insecure manner		X				X		
Deliberate actions to breach data protection or network security rules		X			X	X		
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software		X			X	X		
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature		X	X			X		
Using personal email / social networking / instant messaging / text messaging to carry out digital communications with pupils		X				X		
Actions which could compromise the staff member's professional standing		X	X			X		
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school		X	X			X		
Using proxy sites or other means to subvert the school's filtering system		X			X	X		
Accidentally accessing offensive or pornographic material and failing to report the incident		X				X		
Deliberately accessing or trying to access offensive or pornographic material		X	X	X		X	X	X
Breaching copyright or licensing regulations		X				X		
Continued infringements of the above, following previous warnings or sanctions		X	X	X		X	X	X

9. Acceptable Use Agreement for Staff

Staff ICT Acceptable Use Policy

As a professional organisation with responsibility for children's safeguarding it is important that all staff take all possible and necessary measures to protect data and information systems from infection, unauthorised access, damage, loss, abuse and theft. All members of staff have a responsibility to use the school's computer system in a professional, lawful, and ethical manner. To ensure that members of staff are fully aware of their professional responsibilities when using Information Communication Technology and the school systems, they are asked to read and sign this Acceptable Use Policy.

This is not an exhaustive list and all members of staff are reminded that ICT use should be consistent with the school ethos, other appropriate policies and the Law.

- I understand that Information Systems and ICT include networks, data and data storage, online and offline communication technologies and access devices. Examples include mobile phones, PDAs, digital cameras, email and social media sites**.**

- School owned information systems must be used appropriately. I understand that the Computer Misuse Act 1990 makes the following criminal offences: to gain unauthorised access to computer material; to gain unauthorised access to computer material with intent to commit or facilitate commission of further offences or to modify computer material without authorisation.

- I understand that any hardware and software provided by my workplace for staff use can only be used by members of staff and only for educational use. To prevent unauthorised access to systems or personal data, I will not leave any information system unattended without first logging out or locking my login as appropriate.

- I will respect system security and I will not disclose any password or security information. I will use a 'strong' password (A strong password has numbers, letters and symbols, with 8 or more characters, does not contain a dictionary word and is only used on one system).

- I will not attempt to install any purchased or downloaded software, including browser toolbars, or hardware without permission from the ICT technician.

- I will ensure that any personal data of pupils, staff or parents/carers is kept in accordance with the Data Protection Act 1988. This means that all personal data will be obtained and processed fairly and lawfully, only kept for specific purposes, held no longer than necessary and will be kept private and secure with appropriate security measures in place, whether used in the workplace, hosted online (only within countries or sites with suitable data protection controls) or accessed remotely. No data will be removed from the school site (such as via email or on memory sticks or CDs) Any images or videos of pupils will only be used as stated in the school image use policy Image Use Policy) and will always take into account parental consent.

- I will not keep professional documents which contain school-related sensitive or personal information (including images, files, videos etc.) on any personal devices (such as laptops, digital cameras, mobile phones), unless they are secured and encrypted. Where possible I will upload any work documents and files in a password-protected environment. I will protect the devices in my care from unapproved access or theft.

- I will not store any personal information on the school computer system that is unrelated to school activities, such as personal photographs, files or financial information.

- I will respect copyright and intellectual property rights.

- I have read and understood the school e-Safety policy which covers the requirements for safe ICT use, including using appropriate devices, safe use of social media websites and the supervision of pupils within the classroom and other working spaces (see e-Safety Policy).

- I will report all incidents of concern regarding children's online safety to the Designated Child Protection Coordinators (Dr Pryer and Mrs Cafferty) and/or the e-Safety Coordinator (Dr Pryer) as soon as possible. I will report any accidental access, receipt of inappropriate materials, filtering breaches or unsuitable websites to (Dr Pryer) the e-Safety Coordinator as soon as possible (see attached Reporting an e-safety Incident flowchart and E-safety Incident Report Template).

- I will not attempt to bypass any filtering and/or security system put in place by the school. If I suspect a computer or system has been damaged or affected by a virus or other malware or if I have lost any school related documents or files, then I will report this to the SBM/Headteacher as soon as possible.

- My electronic communications with pupils, parents/carers and other professionals will only take place via work approved communication channels e.g. via a school provided email address or telephone number. Any pre-existing relationships which may compromise this will be discussed with the Senior Leadership team.

- My use of ICT and information systems will always be compatible with my professional role, whether using school or personal systems. This includes the use of email, text, social media, social networking, gaming, web publications and any other devices or websites. My use of ICT will not interfere with my work duties and will be in accordance with the school AUP and the Law.

- Mobile devices will not be used in any areas being used for changing. This includes cloakrooms and toilets. This rule applies to staff, visitors, trustees and pupils.

- I will not create, transmit, display, publish, forward or engage in any material that is likely to harass, cause offence, inconvenience or needless anxiety to any other person, or anything which could bring my professional role, the school, or the County Council, into disrepute.

- I will promote e-Safety with the pupils in my care and will help them to develop a responsible attitude to safety online, system use and to the content they access or create.

- If I have any queries or questions regarding safe and professional practise online either in school or off site, then I will raise them with the e-Safety Coordinator (Dr Pryer).

- I understand that my use of the information systems, Internet and email may be monitored and recorded to ensure policy compliance.

The School may exercise its right to monitor the use of information systems, including Internet access and the interception of e-mails in order to monitor compliance with this Acceptable Use Policy and the School's Data Security Policy. Where it believes unauthorised and/or inappropriate use of the service's information system or unacceptable or inappropriate behaviour may be taking place, the School will invoke its disciplinary procedure. If the School suspects that the system may be being used for criminal purposes or for storing unlawful text, imagery or sound, the matter will be brought to the attention of the relevant law enforcement organisation.

I have read and understood and agree to comply with the Staff ICT Acceptable Use Policy.

Signature: _____ Date: _____

Full Name: _____ (printed)

Job Title: _____

10. Acceptable Use Agreement for Trustees and Visitors

ICT and the related technologies such as email, the internet and mobile devices are an expected part of our daily working life in school. This policy is designed to ensure that all staff are aware of their professional responsibilities when using any form of ICT. All staff are expected to sign this policy and adhere at all times to its contents. Any concerns or clarification should be discussed with Dr Pryer, school e-safety coordinator.

- I will only use the school's email / Internet / Intranet and any related technologies for professional purposes or for uses deemed 'reasonable' by the Head or Governing Body.
- I will comply with the ICT system security.
- I will not give out my own personal details, such as mobile phone number and personal email address, to pupils.
- I will only use the approved, secure email system(s) for any school business.
- I will ensure that personal data (such as data held on SIMS) is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely. Personal data can only be taken out of school or accessed remotely when authorised by the Head or Governing Body.
- I will not install any hardware of software without permission of ICT Technician.
- 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 inline with school policy and with written consent of the parent, carer or staff member. Images will not be distributed outside the school network without the permission of the parent/ carer, member of staff or Headteacher.
- I understand that all my use of the Internet and other related technologies can be monitored and logged and can be made available, on request, to the Headteacher.
- I will support the school approach to online safety and not deliberately upload or add any images, video, sounds or text that could upset or offend any member of the school community
- I will respect copyright and intellectual property rights.
- I will support and promote the school's e-Safety policy and help pupils to be safe and responsible in their use of ICT and related technologies.
- Mobile devices will not be used in any areas being used for changing. This includes cloakrooms and toilets. This rule applies to staff, visitors, governors and pupils.

I have read and understood and agree to comply with the Trustee and Visitor Acceptable Use Policy.

Signature: _____ Date: _____

Full Name: _____ (printed)

Job Title: _____

11. Agreement for KS1 Pupils Acceptable Use

This is how I stay safe when I use computers:

I will keep my passwords secret.

I will only use the computer for things my teacher has told me to.

I will make sure that all the messages I send are polite.

I will tell a teacher if I see something that makes me feel scared or uncomfortable on the screen.

I will not reply to any nasty message or anything that makes me feel uncomfortable.

I will not tell people about myself online (I will not tell them my name, mobile phone number, anything about my home, family, pets and school).

I will never agree to meet a stranger.

I will not put photographs of myself online without asking a teacher.

I know that my teacher can check what I do online and that if I break the rules I might not be allowed to use a computer.

12. Agreement for KS2 Pupils Acceptable Use

Acceptable Use Agreement / e-safety Rules (KS2)

- ✓ I will only use ICT in school for school purposes.
- ✓ I will only open/delete my own files when my teacher has advised me to do so.
- ✓ I will make sure that all ICT contact with other children and adults is responsible, polite and sensible.
- ✓ I will not deliberately look for, save or send anything that could be unpleasant, nasty or against the law. If I accidentally find anything like this I will tell my teacher immediately.
- ✓ I will not give out my own details such as my name, phone number or home address. I will not use the internet to arrange to meet someone.
- ✓ I will be responsible for my behaviour when using ICT because I know that these rules are to keep me safe.
- ✓ I will support the school approach to online safety and not deliberately upload or add any images, video, sounds or text that could upset any member of the school community.
- ✓ I know that my use of ICT can be checked and that my parent/ carer would be contacted if a member of school staff is concerned about my e-safety.

13. Acceptable Use Agreement for KS3 Pupils

Secondary Pupil Acceptable Use (KS3)
Agreement / e-Safety Rules

- I will only use ICT systems in school, including the internet, email, digital video, mobile technologies, etc, for school purposes.
- I will not download or install software on school equipment.
- I will make sure that all ICT communications with pupils or others is responsible and sensible.
- I understand that I am responsible for my behaviour when using the Internet. This includes resources I access and the language I use.
- I will not deliberately browse, download, upload or forward material that could be considered offensive or illegal. If I accidentally come across any such material I will report it immediately to my teacher.
- I will not give out any personal information such as name, phone number or address. I will never arrange to meet anyone including when using multimedia technologies.
- Images of pupils and/ or staff will only be taken, stored and used for school purposes inline with school policy and not be distributed outside the school network without the permission.
- I will ensure that my online activity, both in school and outside school, will not cause my school, the staff, pupils or others distress
- I will support the school approach to online safety and not deliberately upload or add any images, video, sounds or text that could upset or offend any member of the school community
- I will respect the privacy and ownership of others' work on-line at all times.
- I will not attempt to bypass the internet filtering system.
- I understand that all my use of the Internet and other related technologies can be monitored and logged and can be made available to my teachers.
- I understand that these rules are designed to keep me safe and that if they are not followed, school sanctions will be applied and my parent/ carer may be contacted. It may result in a loss of privileges.