Fairlawn

Fairlawn Primary School

Online Safety Policy

Chair of LGB	**Lesley Freed**
Approval date:	**October 2019**
Review date:	**October 2020**

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. These risks include:

- Access to illegal, harmful, or inappropriate images or other content
- Unauthorised access to / loss of / sharing of personal information
- The risk of being subject to grooming by those with whom they make contact on the internet.
- The sharing / distribution of personal images without an individual's consent or knowledge
- Inappropriate communication / contact with others, including strangers
- Cyber-bullying
- Peer on peer abuse
- Grooming
- Sharing locational information when live-streaming
- Access to unsuitable video / internet games
- An inability to evaluate the quality, accuracy, and relevance of information on the internet
- Plagiarism and copyright infringement
- Illegal downloading of music or video files
- The potential for excessive use which may impact on social and emotional development and learn

Online 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's e-safety policy will operate in conjunction with other policies including those for Child Protection, Health and Safety, Behaviour and Anti Bullying. It will be supported by the school's ICT and Personal Social and Health Education (PSHE) curriculum.

The Principal, Mrs Julie Molesworth; the Online Safety Coordinator, Miss Lauren David and the ICT Coordinator, Mrs Siobhan Lennox-Brown are responsible for the production, review and monitoring of the school's Online Safety Policy/documents and practice.

As communications technologies are constantly changing this policy will be reviewed on an annual basis or sooner in response to new practices coming to the school's attention.

Our school's online safety policy has been written from a template provided by South West Grid for Learning.

Policy and Leadership
This section begins with an outline of the key people responsible for developing our Online Safety Policy and keeping everyone safe with ICT. It also outlines the core responsibilities of all users of ICT in our school. It goes on to explain how we maintain our policy and then to outline how we try to remain safe while using different aspects of ICT.

Responsibilities: Online Safety Coordinator
Our online safety coordinator is the person responsible to the Principal and governors for the day-to-day issues relating to online safety.

The Online Safety Coordinator:

• may lead discussions on online safety with the School Council
• takes day to day responsibility for online safety issues and has a leading role in establishing and reviewing the school online safety policies / documents
• ensures that all staff are aware of the procedures that need to be followed in the event of an online safety incident
• provides training and advice for staff
• liaises with school ICT technical staff where necessary
• receives reports of online safety incidents and creates a log of incidents to inform future online safety developments
• reports regularly to Principal

Responsibilities: Governors
Our governors are responsible for the approval of this policy and for reviewing its effectiveness. This will be carried out by the governors (or a governors' subcommittee) receiving regular information about online safety incidents and monitoring reports.

Responsibilities: Principal
The Principal is responsible for ensuring the safety (including online safety) of members of the school community, though the day-to-day responsibility for online safety is delegated to the Online Safety Coordinator. The Senior Management Team is aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff. See flow chart on dealing with online safety incidents – below and relevant Local Authority HR /disciplinary procedures).

Responsibilities: Classroom Based Staff
Teaching and Support Staff are responsible for ensuring that:

- they have an up to date awareness of online safety matters and of the current school online safety policy and practices
- they report any suspected misuse or problems to the Online Safety Co-ordinator

- online safety issues are embedded in the curriculum and other school activities.

Schedule for development / monitoring / review of this policy

The implementation of this online safety policy will be monitored by the:	Online Safety Co-ordinator
Monitoring will take place at regular intervals	Annually
The governing body will receive a report on the implementation of the online safety policy generated by the monitoring group (which will include anonymous details of online safety incidents) at regular intervals	Annually
The online safety policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to online safety or incidents that have taken place.	Annually
Should serious online safety incidents take place, the following external persons / agencies should be informed:	Bristol Safeguarding Children's Board Bristol City Council Police

Policy Scope

This policy applies to all members of the school community (including staff, pupils, volunteers, parents / carers, visitors, community users) who have access to and are users of school ICT systems, both in and out of school.

The Education and Inspections Act 2006 empowers head teachers, to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying or other online safety incidents covered by this policy, which may take place out of school, but are linked to membership of the school.

The school will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents / carers of incidents of inappropriate online safety behaviour that take place out of school.

Acceptable Use Policies

All members of the school community are responsible for using the school ICT systems in accordance with the appropriate acceptable use policy.

Acceptable use policies are provided in Appendix 1 of this policy for:

- Pupils (EYFS + KS1 / KS2)
- Staff (and volunteers)
- Parents / carers (including permissions to use pupil images / work and to use ICT systems)

Illegal or inappropriate activities and related sanctions

The school believes that the activities listed below are inappropriate in a school context (those in bold are illegal) and that users should not engage in these activities when using school equipment or systems (in or out of school). Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:

- **child sexual abuse images (illegal - The Protection of Children Act 1978)**
- **grooming, incitement, arrangement or facilitation of sexual acts against children (illegal – Sexual Offences Act 2003)**
- **possession of extreme pornographic images (illegal – Criminal Justice and Immigration Act 2008)**
- **criminally racist material in UK – to stir up religious hatred (or hatred on the grounds of sexual orientation) (illegal – Public Order Act 1986)**
- pornography
- promotion of any kind of discrimination
- promotion of racial or religious hatred
- threatening behaviour, including promotion of physical violence or mental harm
- any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute

Additionally the following activities are also considered unacceptable on ICT equipment provided by the school:

- Using school systems to run a private business
- Use systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by Bristol City Council and / or the school
- Uploading, downloading or transmitting commercial software or any copyrighted materials belonging to third parties, without the necessary licensing permissions
- Revealing or publicising confidential or proprietary information (eg financial / personal information, databases, computer / network access codes and passwords)
- Creating or propagating computer viruses or other harmful files
- 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
- On-line gambling and non-educational gaming
- Use of personal social networking sites / profiles for non-educational purposes

If members of staff suspect that misuse might have taken place, but that the misuse is not illegal (see above) it is essential that correct procedures are used to investigate, preserve evidence and protect those carrying out the investigation.

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:

Actions / Sanctions

Students / Pupils Incidents	Refer to class teacher / tutor	Refer to Head of Department / Year / other	Refer to Headteacher / Principal	Refer to Police	Refer to technical support staff for action re filtering / security etc.	Inform parents / carers	Removal of network / internet access rights	Warning	Further sanction eg detention /
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).		X	X	X					
Unauthorised use of non-educational sites during lessons	X	X							
Unauthorised / inappropriate use of mobile phone / digital camera / other mobile device	x	X							
Unauthorised / inappropriate use of social media / messaging apps / personal email	x	x	X						
Unauthorised downloading or uploading of files	x	X							
Allowing others to access school / academy network by sharing username and passwords	x	x	x		x	x	x	x	

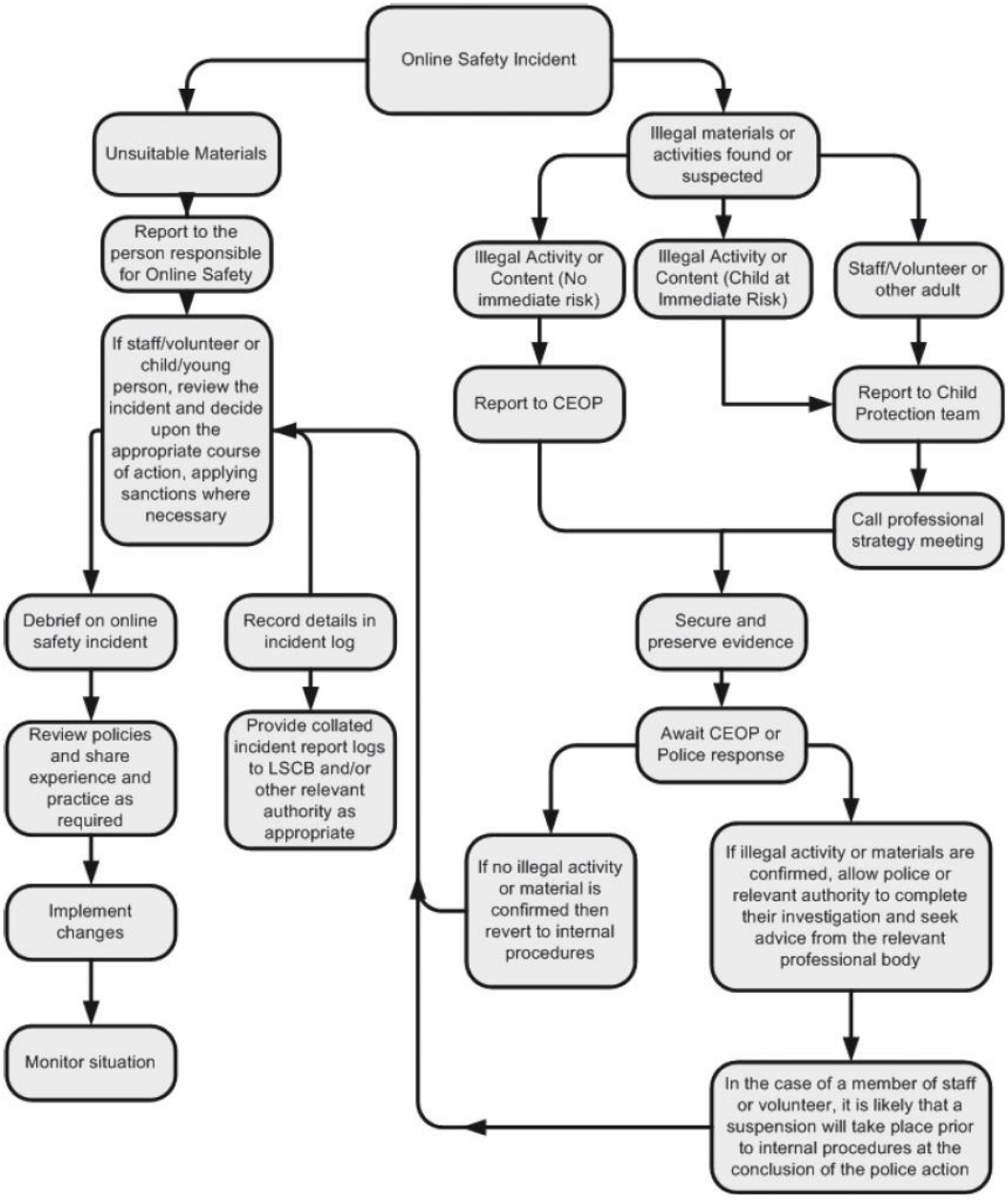
Attempting to access or accessing the school / academy network, using another student's / pupil's account	x	x	x			x	x	X	
Attempting to access or accessing the school / academy network, using the account of a member of staff	x	x	x		x	x	x	x	X
Corrupting or destroying the data of other users	x	x	x		x	x	x	X	X
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature	x	x	x			x	x	x	X
Continued infringements of the above, following previous warnings or sanctions	x	x	x	x		x	x	x	x
Actions which could bring the school / academy into disrepute or breach the integrity of the ethos of the school	x	x	x			x	X		
Using proxy sites or other means to subvert the school's / academy's filtering system	x	x	x		x	x	x	x	X
Accidentally accessing offensive or pornographic material and failing to report the incident	x	x	x	x	x	x	x	x	x
Deliberately accessing or trying to access offensive or pornographic material	x	x	x	x	x	x	x	x	x
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act	x	x	x		x	x	x	x	X

Staff Incidents	Refer to line managerr	Refer to Headteacher	Refer to Local Authority /	Refer to Police	Refer to Technical Support Staff for action re filtering	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	x	
Inappropriate personal use of the internet / social media / personal email	x	x			x	X		
Unauthorised downloading or uploading of files	x	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 e.g. holding or transferring data in an insecure manner	x	x				X		
Deliberate actions to breach data protection or network security rules	x	x			x	x	x	
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software	x	x	x			X	x	X
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature	x	x	x			X	x	
Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with students / pupils	x	x	x			X		X
Actions which could compromise the staff member's professional standing	x	X				X		

Actions which could bring the school / academy into disrepute or breach the integrity of the ethos of the school / academy	x	x				x		
Using proxy sites or other means to subvert the school's / academy's filtering system	x	x			x	x	x	
Accidentally accessing offensive or pornographic material and failing to report the incident	x	x	x	x	x	x	x	x
Deliberately accessing or trying to access offensive or pornographic material	x	x	x	x	x	x	x	x
Breaching copyright or licensing regulations	x	x				x		
Continued infringements of the above, following previous warnings or sanctions	x	x	x			x	x	x

Reporting of online safety breaches

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:



Use of hand held technology (personal phones and hand held devices)

We recognise that the area of mobile technology is rapidly advancing and it is our school's policy to review its stance on such technology on a regular basis. Currently our policy is this:

• Members of staff are permitted to bring their personal mobile devices into school. They are required to use their own professional judgement as to when it is appropriate to use them.

Broadly speaking this is:
Personal hand held devices will be used in lesson time only in an emergency or extreme circumstances. Members of staff are free to use these devices in school, outside teaching time, but not in the presence of children.

• Pupils are not currently permitted to bring their personal hand held devices into school.

Use of digital and video images
When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.

• Members of staff are allowed to take digital still and video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be captured using school equipment; the personal equipment of staff should not be used for such purposes.

• Care should be taken when taking digital / video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.

• Pupils must not take, use, share, publish or distribute images of others without their permission.

Use of web-based publication tools
Our school uses the public facing website, http://www.fairlawn@bristol.sch.uk/ for sharing information with the community beyond our school. This includes, from time-to-time celebrating work and achievements of children.

All users are required to consider good practice when publishing content.

• Personal information should not be posted on the school website and only official email addresses (provided as links rather than appearing directly on the site) should be used to identify members of staff (never pupils).

• Only pupil's first names are used on the website, and only then when necessary.

• Photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with the following good practice guidance on the use of such images: pupils' full names will not be used anywhere on a website or blog, and never in association with

photographs. Parents need to give signed permission before photographs of pupils are published on the school website.

• Pupil's work can only be published with the permission of the pupil and parents or carers.

Online safety Education

Whilst regulation and technical solutions are very important, their use must be balanced by educating pupils to take a responsible approach. The education of pupils in online safety is therefore an essential part of the school's e- safety provision. Children and young people need the help and support of the school to recognise and avoid online safety risks and build their resilience. This is particularly important for helping children to stay safe out of school where technical support and filtering may not be available to them. Therefore, the DfE guidance highlights the importance of focusing on the knowledge and behaviours that help young people to navigate the online world safely and confidently regardless of the app, platform or device they are on.

Knowledge and behaviours include:

- How to evaluate what they see online
- How to recognise techniques used for persuasion
- Understanding acceptable and unacceptable online behaviour
- How to identify online risks
- How and when to seek support, including reporting to CEOP

Online safety education will be provided in the following ways at Fairlawn Primary School:

• A planned online safety programme should be provided as part of ICT, PSHE and other lessons and should be regularly revisited – this will cover both the use of ICT and new technologies in school and outside school.

• We use the resources on CEOP's Think U Know site as a basis for our online safety education http://www.thinkuknow.co.uk/teachers/resources/ *(Hector's World at KS1 and Cyber Cafe at KS2)*

• Key online safety messages should be reinforced through further input via assemblies and pastoral activities as well as informal conversations when the opportunity arises.

• In lessons where internet use is pre-planned, it is best practice that 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.

• Where pupils are allowed to freely search the internet, e.g. using search engines, staff should be vigilant in monitoring the content of the websites the young people visit.

Parent and carer awareness

Many parents and carers have only a limited understanding of online safety risks and issues, yet they play an essential role in the education of their children and in the monitoring and regulation of the children's on-line experiences. Parents often either underestimate or do not realise how often children and young people come across potentially harmful and inappropriate material on the internet and are often unsure about what they would do about it. "There is a generational digital divide". (Byron Report).

The school will therefore seek to provide information and awareness to parents and carers through:

- Letters, newsletters, web site
- Parents evenings
- Reference to the parents materials on the Think U Know website (www.thinkuknow.co.uk) or others

Appendix 1 - Acceptable use policy agreement templates

Acceptable use policy agreement – pupil (KS1)

This is how we stay safe when we use computers at Fairlawn Primary School:

- I will ask a teacher or suitable adult if I want to use the computers / tablets
- I will only use activities that a teacher or suitable adult has told or allowed me to use
- I will take care of the computer and other equipment
- I will ask for help from a teacher or suitable adult if I am not sure what to do or if I think I have done something wrong
- I will tell a teacher or suitable adult if I see something that upsets me on the screen
- I know that if I break the rules I might not be allowed to use a computer / tablet

Signed (child): .....

Signed (parent): ..... Date: .....

Appendix 2 - Acceptable use policy agreement – pupils (KS2)

I understand that while I am a member of Fairlawn Primary School I must use technology in a responsible way.

For my own personal safety:

• I understand that my use of technology (especially when I use the internet) will, wherever possible be supervised and monitored.
• I understand that my use of the internet will be monitored
• I will keep my own personal information safe as well as that of others.
• I will tell a trusted adult if anything makes me feel uncomfortable or upset when I see it online.

For the safety of others:

• I will not interfere with the way that others use their technology.
• I will be polite and responsible when I communicate with others,
• I will not take or share images of anyone without their permission.

For the safety of the school:

• I will not try to access anything illegal.
• I will not download anything that I do not have the right to use.
• I will only use my own personal ICT kit if I have permission and then I will use it within the agreed rules.
• I will not deliberately bypass any systems designed to keep the school safe (such as filtering of the internet).
• I will tell a responsible person if I find any damage or faults with technology, however this may have happened.
• I will not attempt to install programmes on ICT devices belonging to the school unless I have permission.
• I will only use social networking, gaming and chat through the sites the school allows

I understand that I am responsible for my actions and the consequences.

I have read and understood the above and agree to follow these guidelines:

Signed (child): .....

Signed (parent): ..... Date: .....

Appendix 3 - Acceptable Use Policy Agreement - Staff

I understand that I must use school ICT systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the ICT systems and other users.

Keeping Safe

- I know that the school will monitor my use of the ICT systems, email and other digital communications.
- I will only use my own user names and passwords which I will choose carefully so they cannot be guessed easily.
- I will not use any other person's username and password.
- I will ensure that my data is regularly backed up.
- I will not engage in any on-line activity that may compromise my professional responsibilities or compromise the reputation of the school or its members.
- I understand that data protection requires that any personal data that I have access to must be kept private and confidential, except when it is deemed necessary that I am required by law or by school policy to disclose it to an appropriate authority.
- I will only transport, hold, disclose or share personal information about myself or others, as outlined in the school personal data policy. I will not send personal information by e-mail as it is not secure.
- I will not try to bypass the filtering and security systems in place.
- I will only use my personal ICT in school for permissible activities and I will follow the rules set out in this agreement. I will ensure that any such devices are protected by up to date anti-virus software and are free from viruses.
- I will make sure that my equipment is locked in a secure location both when I am on onsite and when I am off site to protect the information on it.

Promoting Safe Use by Learners

- I will model safe use of the internet in school.
- I will educate young people on how to use technologies safely according to the school teaching programme.
- I will take immediate action in line with school policy if an issue arises in school that might compromise learner, user or school safety or if a child reports any concerns.

Communicating

- I will communicate online in a professional manner and tone, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will only communicate with students / pupils and parents / carers using official school systems. Any such communication will be professional in tone and manner.
- I will be aware that any communication could be forwarded to an employer or governors.
- I will only use chat and social networking sites that are approved by the school I will not use personal email addresses on the school ICT systems unless I have permission to do so.

Research and Recreation

- I will not upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others.
- I will not (unless I have permission) make large downloads or uploads that might take up internet capacity.
- I know that all school ICT is primarily intended for educational use and I will only use the systems for personal or recreational use if this is allowed by the school.

Sharing

- I will not access, copy, remove or otherwise alter any other user's files, without their permission.
- I will ensure that I have permission to use the original work of others in my own work and will credit them if I use it.
- Where work is protected by copyright, I will not download or distribute copies (including music and videos).
- I will only take images / video of pupils and staff where it relates to agreed learning and teaching activities and will ensure I have parent/staff permission before I take them.
- If these are to be published online or in the media I will ensure that parental / staff permission allows this.
- I will not use my personal equipment to record images / video unless I have permission to do so.
- I will not keep images and videos of students stored on my personal equipment unless I have permission to do so. If this is the case I will ensure that these images cannot be accessed or copied by anyone else or used for any purpose other than that I have permission for.
- Where these images are published (e.g. on the school website / Merlin) I will ensure it is not possible to identify the people who are featured by name or other personal information.

Buying and Selling

- I will not use school equipment for online purchasing unless I have permission to do so.

Problems

- I will immediately report any illegal, inappropriate or harmful material or incident I become aware of, to the online safety co-ordinator or head teacher.
- I will not install or store programmes on a computer unless I have permission.
- I will not try to alter computer settings, unless this is allowed in school policies.
- I will not cause damage to ICT equipment in school.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.
- I will not open any attachments to emails, unless the source is known and trusted, due to the risk of the attachment containing viruses or other harmful programmes.

I understand that these rules are in place to enable me to use ICT safely and that if I do not follow them I may be subject to disciplinary action. I agree to use ICT by these rules when:

- I use school ICT systems at school or at home when I have permission to do so
- I use my own ICT (when allowed) in school
- I use my own ICT out of school to use school sites or for activities relating to my employment by the school

Staff / Volunteer Name _____

Signed _____

Date _____