North Road Primary School

ICT & E-SAFETY POLICY

Content

Agreed at the School FGB Committee Meeting Thursday 8th December 2016

Signed: ……Rob Broom ……………………… Chair of Governors

Review Date: Autumn 2018

Equalities Impact Assessment: Completed ☒

Introduction

This Policy has been produced based on the model South West Grid for Learning E-Safety policy document that has been adapted for North Road Community Primary School and will consider all current and relevant issues, in a whole school context, linking with other relevant policies, such as the Child Protection, Behaviour and Anti-Bullying policies. The SWGfL Model Policy template that this policy is based on can be found on their website www.swgfl.org.uk/policy and the copyright of this Self Review Framework is held by SWGfL.

Background / Rationale

New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school.

The internet and other digital and information technologies are powerful tools, which open up new opportunities for everyone. Electronic communication helps teachers and pupils learn from each other. These technologies can stimulate discussion, promote creativity and increase awareness of context to promote effective learning. Children and young people should have an entitlement to safe internet access at all times.

The requirement to ensure that children and young people are able to use the internet and related communications technologies appropriately and safely is addressed as part of the wider duty of care to which all who work in schools are bound. A school e-safety policy should help to ensure safe and appropriate use. The development and implementation of such a strategy should involve all the stakeholders in a child's education from the headteacher and governors to the senior leaders and classroom teachers, support staff, parents, members of the community and themselves.

The use of these exciting and innovative tools in school and at home has been shown to raise educational standards and promote pupil achievement.

However, the use of these new technologies can put young people at risk within and outside the school. Some of the dangers they may face 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
- 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 the social and emotional development and learning of the young person.

Many of these risks reflect situations in the off-line world and it is essential that this e-safety policy is used with other relevant school policies eg behaviour, anti-bullying and child protection policies.

As with all other risks, it is impossible to eliminate those risks completely. It is therefore essential, through good educational provision to build students' / pupils' resilience to the risks to which they may be exposed, so that they have the confidence and skills to face and deal with these risks.

The school must demonstrate that it has provided the necessary safeguards to help ensure that they have done everything that could reasonably be expected of them to manage and reduce these risks. The e-safety policy that follows explains how we intend to do this, while also addressing wider educational issues in order to help young people (and their parents/carers) to be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.

Development / Monitoring / Review of this Policy

This e-safety policy has been developed by the:

- Headteacher
- School Business Manager
- E-Safety Governor

The school will monitor the impact of the policy using:

- Logs of reported incidents
- SWGfL monitoring logs of internet activity (including sites visited)
- Surveys / questionnaires of
  - Pupils
  - parents / carers
  - staff

Scope of the Policy

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 Headteachers, 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 e-safety incidents covered by this policy, which may take place out of school, but is linked to membership of the school.

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

Roles and Responsibilities

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

Governors:

Governors are responsible for the approval of the E-Safety Policy and for reviewing the effectiveness of the policy. This will be delegated to an E-Safety Governor who reports to the School Curriculum and Pupils Committee with regular information about e-safety incidents and monitoring reports and policy. The role of the E-Safety Governor will include:

- regular meetings with the ICT Subject Leader
- regular monitoring of e-safety incident logs
- receives reports of e-safety incidents and creates a log of incidents to inform future e-safety developments
- reporting to relevant Governors committee / meeting

Headteacher and Senior Leaders:

- The Headteacher and Senior Leader are responsible for ensuring the safety (including e-safety) of members of the school community.
- The Headteacher / Senior Leader are responsible for ensuring that they and other relevant staff receive suitable CPD to enable them to carry out their e-safety roles and to train other colleagues, as relevant
- The Headteacher and another member of the Senior Leadership Team 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 SWGfL flow chart on dealing with e-safety incidents – included in a later section – “Responding to incidents of misuse” and relevant Local Authority HR / disciplinary procedures)

Headteacher as E-Safety Lead:

- takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policies and documents
- ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place.
- provides training and advice for staff
- liaises with the Local Authority and school ICT technical staff
- meets regularly with E-Safety Governor to discuss current issues, review incident logs and filtering / change control logs

Technical staff
(Administration and Curriculum: South Gloucestershire IT.

The ICT Technician:

- 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 the SWGfL Security Policy and Acceptable Usage Policy.
- that users may only access the school’s networks through a properly enforced password protection policy, in which passwords are regularly changed
- SWGfL is informed of issues relating to the filtering applied by the Grid
- that he / she keeps up to date with e-safety technical information in order to effectively carry out their e-safety role and to inform and update 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 Headteacher.

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 e-safety policy and practices
- they have read, understood and signed the school Staff Acceptable Use Agreement
- they report any suspected misuse or problem to the Headteacher for investigation / action / sanction and also refer, if necessary, to the Whisteblowing Policy.
- digital communications with pupils should be on a professional basis.
- 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 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 person for child protection (Headteacher)
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 Rules for Keeping Safe Agreement, 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 the schools 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 and information about national / local e- safety campaigns / literature. Parents and carers will be responsible for:

- Signing the parent/carer acceptable use Policy Agreement
- Supporting the Pupil Safe Use of ICT Agreement

Policy Statements

Education – pupils

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 e-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 e-safety risks and build their resilience.
E-Safety education will be provided in the following ways:

- A discrete planned e-safety programme (Hector's World) will be delivered annually, alongside teachings of ICT / PHSE / other lessons – this will cover both the use of ICT and new technologies in school and outside school
- Key e-safety messages should be reinforced as part of a planned programme of assemblies
- Pupils should be taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information.
- Pupils should be helped to understand the need for the Pupil Agreement and encouraged to adopt safe and responsible use of ICT, the internet and mobile devices both within and outside school
- Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Rules for use of ICT systems / internet will be posted in the IT suite and each classroom
- Staff should act as good role models in their use of ICT, the internet and mobile devices.

Education – parents / carers

Many parents and carers have only a limited understanding of e-safety risks and issues, yet they play an essential role in the education of their children and in the monitoring / 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, website
- Parents' evenings

Education & Training – Staff

It is essential that all staff receive e-safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- An audit of the e-safety training needs of all staff will be carried out regularly. In response to this a planned programme of formal e-safety training will be made available to staff. It is expected that some staff will identify e-safety as a training need within the appraisal process.
- All new staff should receive e-safety training as part of their induction programme, ensuring that they fully understand the school e-safety policy and Acceptable Use Policies
- The E-Safety Governor, Headteacher and Senior Leader will receive regular updates through attendance at SWGfL / LA / other information / training sessions and by reviewing guidance documents released by BECTA / SWGfL / LA and others.
- This E-Safety policy and its updates will be presented to and discussed by staff in staff meetings.
- The Headteacher will provide advice / guidance / training as required to individuals as required

Training – Governors

Governors should take part in e-safety training / awareness sessions, with particular importance for those who are members of any sub committee / group involved in ICT / e-safety / health and safety / child protection. This may be offered in a number of ways:

- Attendance at training provided by the Local Authority / National Governors Association / SWGfL or other relevant organisation. Updates and information from e-safety Governor.
- Participation in school training / information sessions for staff or parents

Technical – infrastructure / equipment, filtering and monitoring

The school will be responsible for ensuring that the school infrastructure / network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also need to ensure that the relevant people named in the above sections will be effective in carrying out their e-safety responsibilities:

- School ICT systems will be managed in ways that ensure that the school meets the e-safety technical requirements outlined in the SWGfL Security Policy and Acceptable Usage Policy and any relevant Local Authority E-Safety Policy and guidance
- There will be regular reviews and audits of the safety and security of school ICT systems
- Servers, wireless systems and cabling must be securely located and physical access restricted
- All users will be provided with a username and password. There is keep an up to date record of users and their usernames.
- The “master / administrator” passwords for the school ICT system, used by the Network Manager (or other person) must also be available to the Headteacher or other nominated senior leader and kept in a secure place (eg school safe)
- Users will be made responsible for the security of their username and password, must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security.
- The school maintains and supports the managed filtering service provided by SWGfL.
- Any filtering issues should be reported immediately to SWGfL.
- Requests from staff for sites to be removed from the filtered list will be considered by the Headteacher. If the request is agreed, this action will be recorded and logs of such actions shall be reviewed regularly by the E-Safety Governor.
- A log book is in place for users to report any actual / potential e-safety incident to the Headteacher.
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, hand held devices etc from accidental or malicious attempts which might threaten the security of the school systems and data.
- Staff should check with the Headteacher before installing programmes on school workstations / portable devices.
- The school infrastructure and individual workstations are protected by up to date virus software.
- Personal data can not be sent over the internet or taken off the school site unless safely encrypted or otherwise secured. (see School Personal Data Policy Template in the appendix for further detail).

Curriculum

E-safety should be a focus in all areas of the curriculum and staff should reinforce e-safety messages in the use of ICT across the curriculum.

- 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, eg using search engines, staff should be vigilant in monitoring the content of the websites the young people visit.
- Pupils should be taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information
- Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.

Use of digital and video images - Photographic, Video

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff and pupils need to be aware of the risks associated with sharing images and with posting digital images on the internet. Those images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. There are many reported incidents of employers carrying out internet searches for information about potential and existing employees. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- 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 eg on social networking sites.
- Staff are allowed to take digital / video images to support educational aims, but must follow school guidelines concerning the sharing, distribution and publication of those images. Those images should only be taken on 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
- Photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with good practice guidance on the use of such images.
- Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs.
- Written permission from parents or carers will be obtained 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.

Data Protection

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 which states that personal data must be:

- Fairly and lawfully processed
- Processed for limited purposes
- Adequate, relevant and not excessive
- Accurate
- Kept no longer than is necessary
- Processed in accordance with the data subject's rights
- Secure
- Only transferred to others with adequate protection.

Staff must ensure that they:

- At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.
- Use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data.
- Transfer data using encryption and secure password protected devices.

When personal data is stored on any portable computer system, USB stick or any other removable media:

- the data must be encrypted and password protected
- the device must be password protected (many memory sticks / cards and other mobile devices cannot be password protected)
- the device must offer approved virus and malware checking software

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/with permission	Allowed for selected staff	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 photos on mobile phones				X				X
Use of hand held devices eg PDAs, PSPs		X						X
Use of personal email addresses in school, or on school network			X					X
Use of school email for personal emails	X							X
Use of chat rooms / facilities				X				X
Use of instant messaging		X				X		
Use of social networking sites				X				X
Use of blogs		X				X		

When using communication technologies the school considers the following as good practice:

- The official school email service may be regarded as safe and secure and is monitored. Staff should therefore use only the school email service to communicate with others when in school, or on school systems (eg by remote access).
- Users need to be aware that email communications may be monitored
- Users must immediately report, to the nominated person – in accordance with the school policy, the receipt of any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature and must not respond to any such email.
- Any digital communication between staff and pupils or parents / carers (email, chat, etc) must be professional in tone and content. These communications may only take place on official (monitored) school systems. Personal email addresses, text messaging or public chat / social networking programmes must not be used for these communications.
- Pupils should be taught about email safety issues, such as the risks attached to the use of personal details. They should also be taught strategies to deal with inappropriate emails and be reminded of the need to write emails clearly and correctly and not include any unsuitable or abusive material.
- Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff.

Unsuitable / inappropriate activities

The school believes that the activities referred to in the following section would be inappropriate in a school context and that 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:

User Actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
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					X
	promotion or conduct of illegal acts, eg under the child protection, obscenity, computer misuse and fraud legislation					X
	adult material that potentially breaches the Obscene Publications Act in the UK					X

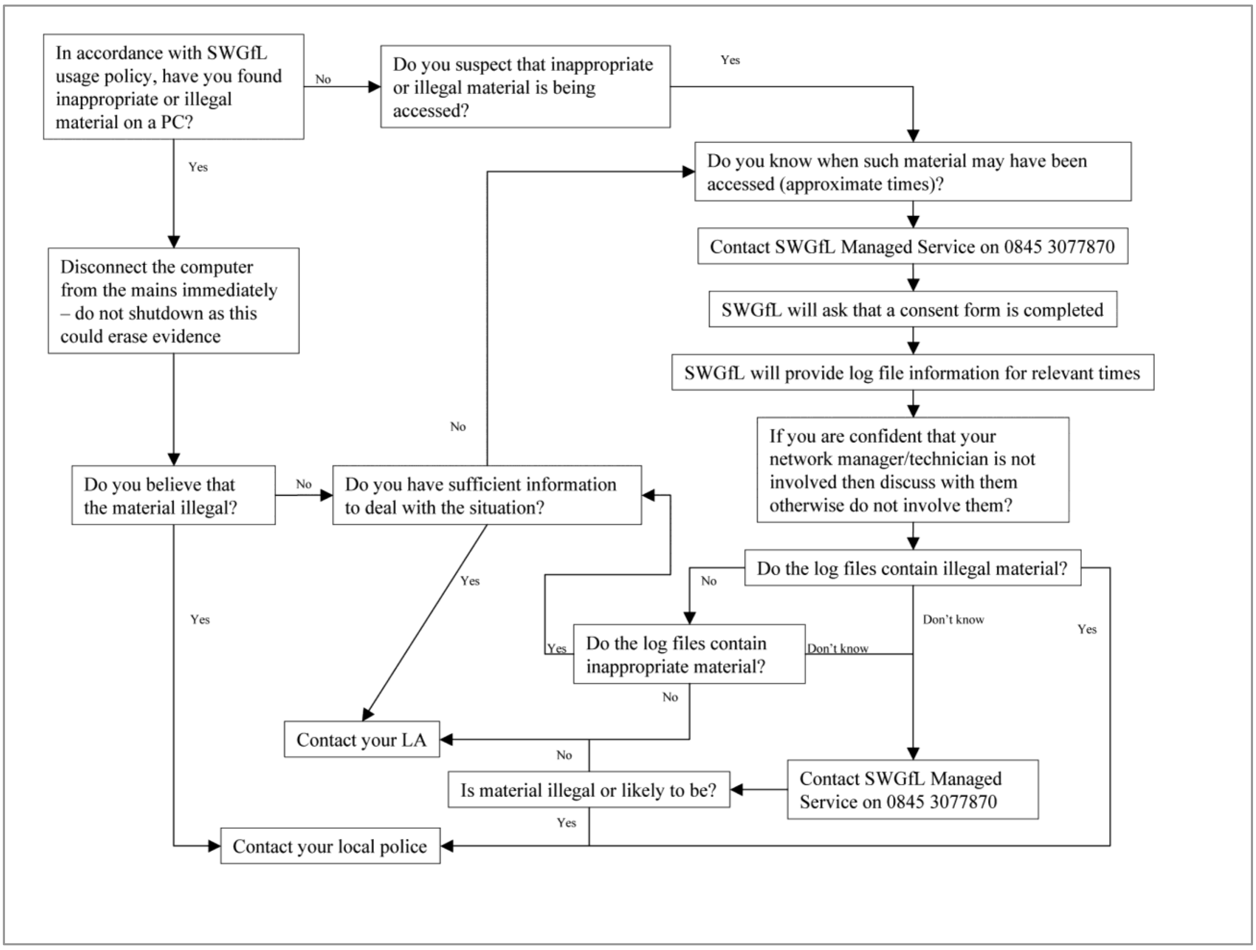
	criminally racist material in UK					X
	pornography				X	
	promotion of any kind of discrimination				X	
	promotion of racial or religious hatred				X	
	threatening behaviour, including promotion of physical violence or mental harm				X	
	any other information which may be offensive to colleagues or 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 SWGfL and / or the school					X	
Uploading, downloading or transmitting commercial software or any copyrighted materials belonging to third parties, without the necessary licensing permissions					X	
Revealing or publicising confidential or proprietary information (eg financial / personal information, 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					X	
Use of video broadcasting eg Youtube			X			

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 any apparent or actual misuse appears to involve illegal activity ie.

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

the SWGfL flow chart – below and http://www.swgfl.org.uk/safety/default.asp should 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.


In accordance with SWGfL usage policy, have you found inappropriate or illegal material on a PC?
No
Do you suspect that inappropriate or illegal material is being accessed?
Yes
Yes
Do you know when such material may have been accessed (approximate times)?
Disconnect the computer from the mains immediately – do not shutdown as this could erase evidence
Contact SWGfL Managed Service on 0845 3077870
SWGfL will ask that a consent form is completed
SWGfL will provide log file information for relevant times
No
If you are confident that your network manager/technician is not involved then discuss with them otherwise do not involve them?
Do you believe that the material illegal?
No
Do you have sufficient information to deal with the situation?
Do the log files contain illegal material?
Yes
No
Yes
Don't know
Yes
Yes
Do the log files contain inappropriate material?
Don't know
No
Contact your LA
No
Is material illegal or likely to be?
Contact SWGfL Managed Service on 0845 3077870
Yes
Contact your local police

If members of staff suspect that misuse might have taken place, but that the misuse is not illegal (as above) it is essential that correct procedures are used to investigate, preserve evidence and protect those carrying out the investigation. In such event the SWGfL "Procedure for Reviewing Internet Sites for Suspected Harassment and Distress" should be followed. This can be found on the SWGfL Safe website within the "Safety and Security booklet". This guidance recommends that more than one member of staff is involved in the investigation which should be carried out on a "clean" designated computer.

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:

Pupils

Incidents:	Refer to class teacher / tutor	Refer to Headteacher	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 / 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	X
Unauthorised use of non-educational sites during lessons	X	X						
Unauthorised use of mobile phone / digital camera / other handheld device		X			X	X		
Unauthorised use of social networking / instant messaging / personal email		X			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 student's / pupil's account		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	X	
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature		X	X		X	X	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			X		X	
Using proxy sites or other means to subvert the school's filtering system		X		X				
Accidentally accessing offensive or pornographic material and failing to report the incident		X			X		X	
Deliberately accessing or trying to access offensive or pornographic material		X			X			X
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act		X			X		X	

Staff (including work experience and students) Actions / Sanctions

Incidents:	Refer to line manager	Refer to Headteacher	Refer to Local Authority / HR	Refer to Police	Refer to Technical Support Staff for action re filtering etc	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				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		
Careless use of personal data eg		X				X		

holding or transferring data in an insecure manner								
Deliberate actions to breach data protection or network security rules		X	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
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature		X				X	X	X
Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with pupils		X	X	X		X	X	X
Actions which could compromise the staff member's professional standing		X				X	X	X
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school		X				X	X	X
Using proxy sites or other means to subvert the school's filtering system		X	X			X	X	X
Accidentally accessing offensive or pornographic material and failing to report the incident		X	X			X		
Deliberately accessing or trying to access offensive or pornographic material		X				X	X	X
Breaching copyright or licensing regulations	X							X
Continued infringements of the above, following previous warnings or sanctions		X						X

Appendices
Can be found on the following pages:

- Pupil Rules for Keeping Safe Agreement
- Parents / Carers Acceptable Usage Policy Agreement
- Staff and Volunteers (including work experience and placement students) Acceptable Usage Policy Agreement
- School Data Protection Policy

North Road Community Primary School
Rules for Keeping Safe with ICT

Keeping Safe

I will not use ICT in school (including my own) without permission from my teacher.

I will choose my user names and passwords carefully to protect my identity and I will not share them.

I will not ask computers to remember my password.

I must keep my personal details and those of others private.

I will not visit unsafe sites or register for things I am not old enough for.

I will log off sites when I have finished.

Communicating

I know that I need to be polite and friendly online.

I know that others may have different opinions and that I should respect them.

I am careful about what I send as messages can be forwarded on to my parents or head teacher.

I know that I must have permission to communicate online and will make sure my teacher / parents know who I communicate with.

I will talk to an adult if an online friend wants to meet me and never arrange to meet anyone without permission.

I will not open messages if the subject field is not polite or if I do not know who it is from.

Research and Fun

I will use clear search words so that I find the right information.

I know that some content may not be filtered out.

I will double check information I find online.

Sharing

I will not use anyone else's work or files without permission.

Where work is protected by copyright, I will not try to download copies.

I will not take or share pictures of anyone without their permission.

I know that anything I put up on the internet can be read be anyone.

Buying and Selling

I can tell if a site is trying to sell something.

I know that I should not buy anything on line without permission.

Problems

I will not try to change computer settings or install programmes.

I will tell a teacher if I find anything on a computer or message that is unpleasant or makes me feel uncomfortable.

I will not damage equipment and will tell a teacher if equipment is broken or not working.

I agree to use ICT by these rules when:

I use school ICT or my own in school (when allowed)

I use my own ICT out of school to use school sites

My Name is

My Class teacher is

Signed Date

North Road Community Primary School

Parent / Carer Acceptable Use Policy Agreement

New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school. Technologies open up new learning opportunities for everyone. They can stimulate discussion, promote creativity and effective learning, and promote more effective communications between parents / carers and the school in order to support young people with their learning. Young people should have an entitlement to safe internet access.

This Acceptable Use Policy is intended to ensure:

- All young people will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- School ICT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- Parents and carers are aware of the importance of e-safety and are involved in the education and guidance of young people with regard to their on-line behaviour.

The school will try to ensure that students have good access to ICT to enhance their learning and will, in return, expect the students to agree to be responsible users. A copy of the Student / Pupil Acceptable Use Policy is attached to this permission form, so that parents / carers will be aware of the school expectations of the young people in their care.

Parents are requested to sign the permission form below to show their support of the school in this important aspect of the school's work.

Permission Form

Parent / Carers Name

Student / Pupil Name

As the parent / carer of the above student, I give permission for my son / daughter to have access to the internet and to ICT systems at school.

I know that my son / daughter has signed an Acceptable Use Agreement and has received, or will receive, e-safety education to help them understand the importance of safe use of ICT – both in and out of school.

I understand that the school will take every reasonable precaution, including monitoring and filtering systems, to ensure that young people will be safe when they use the internet and ICT systems. I also understand that the school cannot ultimately be held responsible for the nature and content of materials accessed on the internet and using mobile technologies.

I understand that my son's / daughter's activity on the ICT systems will be monitored and that the school will contact me if they have concerns about any possible breaches of the Acceptable Use Policy.

Use of Digital / Video Images

The use of digital / video images plays an important part in learning activities. Students / Pupils and members of staff may use the school digital cameras to record evidence of learning and activities. These images may then be used in presentations in subsequent lessons or to celebrate success through their publication in newsletters, on the school website and occasionally in the public media. Staff are not allowed to take photographs using a mobile phone or their own camera.

The school will comply with the Data Protection Act and request parents / carers permission before taking images of members of the school. We will also ensure that when images are published the young people cannot be identified by the use of their names.

Parents are requested to sign the permission form below to allow the school to take and use images of their children.

Permission Form

Parent / Carers Name

Student / Pupil Name

As the parent / carer of the above student / pupil, I agree to the school taking and using digital / video images of my child / children. I understand that the images will only be used to support learning activities or in publicity that reasonably celebrates success and promotes the work of the school.

I agree that if I take digital or video images at, or of, school events which include images of children, other than my own, I will abide by these guidelines in my use of these images.

Signed Date

Home Use of the Internet

We hope you will reinforce the issues contained in the Student Acceptable Use Policy when your child uses the internet at home. In order to do this we recommend that you:

Ensure that children access the internet in a communal room.

Ensure appropriate supervision for the age of your child including supervising all use of the internet by younger users.

Set appropriate rules for using the ICT and the internet safely at home. The school rules could provide a starting point.

Inform the school if you have concerns that the school could help to address through teaching.

Ask your child about the sites they are visiting.

Ensure that family computers are password protected and have robust anti-virus software which is regularly updated.

Ensure content is appropriately filtered for younger users.

Ensure that your child knows that any protection system does not stop all unsafe content and that they need to tell you if they access something inappropriate or get an upsetting message.

Reassure your child that if they talk to you about a problem they are having on the internet you will not ban them from using it as this will discourage them from telling you.

Ensure that your child knows not to leave computers logged on with their user name or logged on to sites with personal details entered as others could use them.

In order to support those parents who may be less familiar with use of the internet we have listed a variety of additional measures that you could take at home to support your child's safe use of the internet.

Additional Guidance on Safe Use of ICT at Home

Keeping Safe

Discuss user names with children and talk about how to choose them carefully to protect their identity.

Talk to young people about the information they should keep private in order to prevent them being contacted or traced including full name, address, telephone no, school, places they do regularly.
Talk to young people about the need to limit access to their own information by using the safety and privacy features of sites to only give access to people they know and being careful who they add as friends.
Model safe behaviour in your use of ICT.

Research and Fun on the internet
Talk to your child about the fact that any information published on the web can be read by anyone and that they should only publish information they would be happy for anyone to read.
Check information that younger users are publishing on the web before it is posted to ensure that they are not putting themselves at risk.
Check that they are old enough for the sites they are using.

Communicating
Discuss the need for young people to be polite to others online and that they should not use bad language or comments which might upset others.
Discuss the fact that e-mails / messages can be intercepted and forwarded on to anyone (including parents, head teacher or future employer!).
Ensure that young people know they should not open messages if the subject field contains anything offensive or if they do not recognise who it is from and that the safest thing to do is to delete it without opening it.
Recognise that there is a difference between online friends who you will never meet and real world friends. Talk to your child about their online friends.
Remind your child that people they talk to online may not be who they seem.

Sharing
Ensure your child knows that downloading games and music that is copyrighted without paying for it is illegal

Buying and Selling Online
Help young people to tell the difference between web sites for information and web sites selling things.
Discuss how to recognise commercial uses of the internet e.g. I Tunes, mobile phone downloads, shopping.
Remind young people that if an offer looks too good to be true it probably is and that they should not respond to unsolicited online offers.
Remind young people that they should not purchase or download anything that costs money without asking permission and that they should not use someone else's identity to buy things online.

Problems
Ensure that they know that if they receive an offensive or worrying message / e-mail they should not reply but should save it and tell you.

North Road Community Primary School

Staff (and Volunteer) Acceptable Use Policy Agreement

The internet and other technologies are powerful tools, which open up new opportunities for everyone. They can stimulate discussion, promote creativity and promote effective learning. They also bring opportunities for staff to be more creative and productive in their work. All users should have an entitlement to good, safe access to ICT and the internet. This Acceptable Use Policy is intended to ensure that:
Staff and volunteers are responsible users and stay safe while using technologies for educational, personal and recreational use.
School ICT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
Staff are protected from potential risk from the use of ICT in their everyday work and work to ensure that young people in their care are safe users.

Acceptable Use Policy Agreement

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. I will not send personal information by e-mail as it is not secure.
Where personal data is transferred outside the secure school network, it must be encrypted.
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.

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.
I will not use my mobile phone or camera to take images in school.
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.
Where these images are published (e.g. on the school website) 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 e-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