NORTH ROAD COMMUNITY PRIMARY SCHOOL

E-Safety Policy

November 2023 Edition

Author/Person Responsible	Sarah Stillie North Road Primary School
Date of Ratification	October 2023
Review Group	C&P Committee - 31st October 2023
Ratification Group	C&P Committee - 31st October 2023
Review Frequency	Annually
Review Date	November 2023
Previous Review Amendments/Notes	Updated in line with LA and NSPCC Guidance/Advice
Related Policies	• Safeguarding Policy • Allegations against staff and volunteers • Staff Code of conduct • Anti-bullying Policy • Photography and Image sharing guidance.
Chair of Governor's Signature	

Equality Impact Assessment (EIA) Part 1: EIA Screening

Policies, Procedures or Practices:	E Safety	Date:	November 2023
EIA Carried Out By:	S Stillie	EIA Approved By:	S Rigby

Groups that may be affected:

Are there concerns that the policy could have a different impact on any of the following groups? (please tick the relevant boxes)	Existing or potential adverse impact	Existing or potential for a positive impact
Age (young people, the elderly; issues surrounding protection and welfare, recruitment, training, pay, promotion)		X
Disability (physical and mental disability, learning difficulties; issues surrounding access to buildings, curriculum and communication)		X
Gender reassignment		X
Marriage and civil partnership		X
Pregnancy and maternity		X
Race		X
Religion and belief (practices of worship, religious or cultural observance, including non-belief)		X
Gender identity		X
Sexual orientation		X

Any adverse impacts are explored in a Full Impact Assessment.

NORTH ROAD COMMUNITY PRIMARY SCHOOL
E-Safety Policy
November 2023

The purpose of this policy statement

North Road Community Primary School works with children and families as part of its activities.

The purpose of this policy statement is to:
• ensure the safety and wellbeing of children and young people is paramount when adults, young people or children are using the internet, social media or mobile devices
• provide staff and volunteers with the overarching principles that guide our approach to online safety
• ensure that, as an organisation, we operate in line with our values and within the law in terms of how we use online devices. The school and governors are committed to the safekeeping of all children who attend the school, and recognise their responsibility for Child Protection.

The policy statement applies to all staff, volunteers, children and young people and anyone involved in North Road Community Primary School's activities.

This E Safety policy has been developed, and will be reviewed and monitored, by our Curriculum and Pupils Committee, including our headteacher. We have also consulted with teaching staff, support staff and the ICT subject leader. The school council has also been consulted for their views. Parents will be made aware of our e-safety policy through our website.

Legal framework

This policy has been drawn up on the basis of legislation, policy and guidance that seeks to protect children in England. Summaries of the key legislation and guidance are available on:
• online abuse
• bullying
• child protection.

We believe that:

• children and young people should never experience abuse of any kind
• children should be able to use the internet for education and personal development, but safeguards need to be in place to ensure they are kept safe at all times.

We recognise that:

• the online world provides everyone with many opportunities; however it can also present risks and challenges
• we have a duty to ensure that all children, young people and adults involved in our organisation are protected from potential harm online
• we have a responsibility to help keep children and young people safe online, whether or not they are using North Road Community Primary School's network and devices
• working in partnership with children, young people, their parents, carers and other agencies is essential in promoting young people's welfare and in helping young people to be responsible in their approach to online safety

• all children, regardless of age, disability, gender reassignment, race, religion or belief, sex or sexual orientation, have the right to equal protection from all types of harm or abuse.

We will seek to keep children and young people safe by:

• appointing an online safety coordinator. For our school this is Sarah Stillie, Headteacher.
• providing clear and specific directions to staff and volunteers on how to behave online through our behaviour code for adults
• supporting and encouraging the young people using our service to use the internet, social media and mobile phones in a way that keeps them safe and shows respect for others
• supporting and encouraging parents and carers to do what they can to keep their children safe online
• developing an online safety agreement for use with young people and their parents or carers
• developing clear and robust procedures to enable us to respond appropriately to any incidents of inappropriate online behaviour, whether by an adult or a child or young person
• reviewing and updating the security of our information systems regularly
• ensuring that user names, logins, email accounts and passwords are used effectively
• ensuring personal information about the adults and children who are involved in our organisation is held securely and shared only as appropriate
• ensuring that images of children, young people and families are used only after their written permission has been obtained, and only for the purpose for which consent has been given
• providing supervision, support and training for staff and volunteers about online safety
• examining and risk assessing any social media platforms and new technologies before they are used within the organisation.

If online abuse occurs, we will respond to it by:

• having clear and robust safeguarding procedures in place for responding to abuse (including online abuse)
• providing support and training for all staff and volunteers on dealing with all forms of abuse, including bullying or cyberbullying, emotional abuse, sexting, sexual abuse and sexual exploitation
• making sure our response takes the needs of the person experiencing abuse, any bystanders and our organisation as a whole into account
• reviewing the plan developed to address online abuse at regular intervals, in order to ensure that any problems have been resolved in the long term.

Monitoring and Review

The school will monitor the impact of the policy through an analysis of:

- Logs of reported incidents and responses
- Monitoring logs of internet activity and any network monitoring data
- Surveys / questionnaires of students, parents / carers, and staff including non-teaching staff
- Monitoring information about the teaching programme and coverage within the curriculum
- Regularly checking that pupils and staff are clear about how to report incidents and respond to them
- The content of the web site is regularly monitored by the headteacher and governors to ensure that it complies with this policy and the acceptable use policies.

Roles and Responsibilities

These are clearly detailed (see appendix i) for all members of the school community.

- The governors have overall responsibility for ratifying the policy, ensuring that it is implemented and monitoring it. This action is delegated to the Curriculum and Pupils Committee.
- The headteacher is responsible for ensuring the safety (including online safety) of members of the school community and the day-to-day responsibility for online safety. The headteacher is also the designated person for child protection and is trained in online safety issues and 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 and cyber-bullying.

Training

There is a planned programme of online safety training for **all** staff and governors to ensure that they understand their responsibilities, as outlined in this, and the acceptable use policies. The following actions are undertaken to raise awareness:

- An audit of the online safety training needs of all staff is carried out annually.
- The headteacher receives regular updates through attendance at relevant training such as LA training sessions and by receiving regular online safety updates from the South Gloucestershire Traded Services.
- All staff, including support staff, have the online safety update newsletter forwarded to them each month.
- Any reported incidents and how they are addressed are discussed at staff meetings and used as an opportunity to test our processes and update staff on how to deal with issues.
- The headteacher provides advice/guidance and training as required to individuals and seeks LA advice on issues where appropriate.

Induction Processes

- All new staff receive online safety training as part of their induction programme.
- Parents of new reception children receive a briefing about online safety and processes when their child starts school. There are also updates to this throughout the key stages.
- Parents of children who join school mid-year are made aware of the processes and their children are introduced to the acceptable use policy.

Teaching and Learning

Online safety is a statutory part of the programme of study for all key stages. Rules and technical solutions are not infallible and we are aware that outside school children will be using unfiltered internet provision. We believe it is crucial to educate children about how to behave responsibly online and how to keep themselves and others safe. Children and young people need the help and support of the school and parents to recognise and avoid online safety risks. There is a planned and progressive scheme of work for online safety, which is taught at every year group. This is based around the Switched on Computing, CEOP Hector's World, Google Be Internet Legends and Digital Literacy Curriculum by SWGfL and, across the key stages, covers:

- Internet safety
- Privacy and security
- Relationships and communication
- Cyberbullying

- Information literacy
- Self-image and identity
- Digital footprint and reputation
- Creative credit and copyright

The scheme of work is delivered as part of computing, PSHE and across our creative curriculum. Regular opportunities are taken to reinforce online safety messages in all lessons and to teach pupils to be critically aware and consider the accuracy of the information they access online. Online safety messages are also reinforced through other subjects and through a planned programme of other activities such as assemblies and events. Older pupils are taught to acknowledge the source of information and respect copyright. Pupils are helped to understand the Acceptable Use Policy, recognise online safety risks, adopt safe practices, report any issues and keep evidence to support reporting (for older children). Staff model safe practice in use of technologies and mobile devices and guide students to appropriate sites and follow practices for dealing with unsuitable material found in internet searches. Where pupils undertake searching of the internet staff monitor the content of the websites they are visiting. If they identify pupils who may be vulnerable, for example, who are not adopting safe practices or completing inappropriate searches, this should be logged and appropriate support given to those pupils to help them understand the risks and what to do to keep safe.
If there are educational reasons why a blocked site is needed for learning then staff can request that this be made available to technical staff. Where this is done this a clearly logged with reasons given for this access.
Children new to the school are provided with an overview of expectations when they start. Annual online safety events such as Safer Internet Day are also used to raise awareness.

Rules for Keeping Safe

These are reinforced through the following:

- Pupils sign an acceptable use agreement (see appendix ii) and this is communicated to parents who we hope will reinforce the messages at home through signing a Parent's Agreement (see appendix iii).
- Pupils are helped to understand the student acceptable use policy and school rules for online safety and encouraged to act accordingly.
- All classes have online safety rules displayed in their classroom and staff regularly refer to these, for example, during activities where children are searching the internet for information. Rules are also displayed in other areas where ICT is used.
- Staff act as good role models in their own use of ICT.
- Staff are aware that there may be some children that are more vulnerable than others to being approached online and endeavour to ensure that these children understand the issues involved.
- Online behaviour is dealt with in accordance with our behaviour policy. There are sanctions and rewards in place for this.

Education – Parents /Carers and the Community

Parents and carers have an essential role in educating their children and monitoring their behaviour online, however they may have a limited understanding of the risks and issues and underestimate the dangers or be unsure how to deal with them. The school aims to raise awareness and support parents through:

- Curriculum activities
- Letters and newsletters including information on any online safety issues that have been raised in school (anonymously recorded) and how to address these

- Parents / carers information meetings
- Events such as Safer Internet Day
- Visits from external agencies
- Providing information and web links about where to access support on the website

Parents of children new to the school are provided with an overview of expectations linked to relevant policies including online safety when their child starts school.

Education – Staff and Volunteers

All staff receive regular online safety training so that they understand the risks and their responsibilities. This includes:

- A planned programme of online safety training which is regularly updated, reinforced, and linked to the expectations outlined in this policy, Keeping Children Safe in Education and in the Ofsted framework.
- All staff sign an acceptable use agreement (see appendix iv)
- An audit of online safety training needs of staff is carried out regularly.
- All new staff receive online safety training and training on relevant policies and expectations as part of their induction programme.
- The headteacher receives regular updates and external training to support them to do their role.
- Policies relevant to online safety and their updates are discussed in staff meetings.
- The headteacher provides regular guidance and training to support individuals where required.

Training – Governors

Governors take part in online safety training and awareness raising sessions, particularly those governors who are involved with technology and safeguarding. This is offered through:

- Attendance at local authority or regional events
- Attendance at relevant staff training
- Regular newsletter information and access to website information

Self-evaluation and Improvement

The school undertakes self-evaluation in order to inform actions to continually improve online safety provision through the following:

- Local authority safeguarding audit
- 360Safe online review
- Surveys with pupils and staff

Password Access to Systems

All our systems are accessed via an individual log in. Users have passwords that include upper and lower case and a number and are encouraged to change these regularly. **Users are told that passwords must never be shared for any IT system and that they are responsible for any actions taking using their log in**. The same log in is used to access our governor online area, computing scheme of work and learner area. Access to systems is through groups so that only the relevant group of users can access a resource.

Internet Provider and Filtering

Integra IT provides North Road Community Primary School's internet service and this includes a filtering service to limit access to unacceptable material for all users.
Internet access and illegal content (child sexual abuse images) is filtered by actively employing the Internet Watch Foundation CAIC list. Content lists are regularly updated and internet use is logged and regularly monitored. However, we are aware that no filtering is completely infallible and consequently focus on teaching pupils to keep safe through our curriculum and teaching. There are two different levels of filtering which are targeted towards different user groups. Consequently, teacher and staff users have access to some resources for teaching that are filtered for learners to ensure that "over blocking" does not restrict teaching.

Technical staff monitor internet traffic and report any issues to schools. The school reports issues through logging a call to the service desk at 3838. Any filtering requests for change and issues are also reported immediately to the South Gloucestershire (Integra IT) technical team on 3838. Requests from staff for sites to be removed from the filtered list must be approved by the headteacher and this is logged and documented by a process that is agreed by the headteacher.

The school are currently implementing a technical monitoring solution through the local authority in order to fulfil the requirements within Keeping Children Safe in Education. The iBoss solution being implemented provides the following:

- active monitoring and automatic alerts for the school to act upon, together with pro-active monitoring by Integra Schools IT to support the school by drawing attention to concerning behaviours, communications or access
- enhanced filtering integrated with the police assessed list of unlawful terrorist content, produced on behalf of the Home Office
- delegated access to the filtering system allows us to permit or deny access to specific content to support the requirement that "over blocking" does not lead to unnecessary restrictions on what can be taught relating to online teaching and safeguarding - the most severe content will always be filtered
- network level filtering which does not rely on any software on the users' devices which could be disabled
- ability to produce reports on the websites visited by all young people and adults using our systems
- the ability for alerts to be set so that a number of people are informed when they are triggered meaning that monitoring does not need to fall into the remit of only one person which could result in issues being missed or covered up
- external alerts to people outside the school (such as safeguarding, online safety officers or IT technicians) so that monitoring is not reliant wholly on school staff and appropriate actions can be taken immediately to safeguard children and staff
- automated reporting to ensure that processes are followed without fail
- ability to log in from anywhere to see reports via web interface

Technical Staff - Roles and Responsibilities

Where the local authority (Integra IT) provides technical support, the "administrator" passwords for the school are not held by the school and the local authority are responsible for their security and any implications of their use.

The school ensures, when working with our technical support provider that the following guidelines are adhered to.

- There are regular reviews and audits of the safety and security of school ICT systems.
- Servers, wireless systems and cabling are securely located and physical access is restricted.
- All users have clearly defined access rights to school ICT systems and are provided with a username and password by the technical support provider.
- Users are 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.
- An agreed policy is in place (using a zip account) for the provision of temporary access of "guests" (e.g. trainee teachers, visitors) onto the school system.
- School ICT technical staff regularly monitor and record the activity of users on the school ICT systems and users are made aware of this in the Acceptable Use Policy.
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, workstations etc. from accidental or malicious attempts, which might threaten the security of the school systems and data.
- The school infrastructure and individual workstations are protected by up to date virus software.
- Only the technician has permissions to install executable files or programmes.
- Any school device (e.g. laptops) can be used off the school premises, but should only be used by the member of staff themselves.
- Any removable media containing confidential information must be password protected.

Use of Digital Images and Video

Ease of access to technologies that take digital images and video has many benefits for learning. Taking and sharing images and video are much easier and, if not managed, this could increase the potential risk of misuse and has the potential to be used for cyberbullying. The school informs and educates users about the risks associated with digital images and these are outlined in the acceptable use policies:

- When using digital images, staff educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images including publishing their own images on social networking sites.
- Pupils should not take, use, share, publish or distribute images / video of others without their permission and staff reinforce this when appropriate.
- Written permission is obtained from parents or carers before photographs of pupils are taken. These photographs are only taken to be used for educational purposes or to promote achievements or the school.
- Staff are allowed to take digital / video images to support educational aims, but follow guidance in the acceptable use policy concerning the sharing, distribution and publication of those images.
- Staff sign permission forms to say that they allow their image to be used for promoting the school and are aware of the risks of this being copied
- Images are only taken and used of individuals where there is a signed permission form in place.
- Pupils full names are not published on any online platform or school communication including the web site, newsletter or twitter feed. Photographs published anywhere that include pupils are carefully selected and not used in association with pupils' full names or other information that could identify them.

- Care is always taken to ensure that pupils are appropriately dressed if images are taken and that they are not participating in any activity that might bring individuals or the school into disrepute.
- In accordance with guidance from the Information Commissioner's Office, parents / carers are welcome to take videos and digital images of their children at school events for their own personal use, as this is not covered by the Government Data Protection Regulations. However, in order to protect other children and respect privacy these images should not be published or made publicly available on social networking sites. Parents / carers should also not comment on any activities involving other pupils in the digital / video images.
- Pupils' work is only published with the permission of pupils and parents / carers.

Mobile Technologies

These might include mobile phones, tablets or any other device that has the capability of accessing the school's wireless network. The primary use of these in school is to support learning, teaching and management.

Children are not allowed to use their personal devices in school as the school provides access to the technologies to be used for learning. If children bring phones into school, they should be left in the office until the end of the school day.

Staff are not allowed to use their personal mobile phones in school while they are teaching and any use should be restricted to times when children are not present. The only exception to this is in case of emergency during a school trip.

Staff are discouraged from using their own mobile phone to take images of children, for example, on a school trip but should use one of the school cameras. If an image is taken on a mobile phone for the purposes of the school Twitter Feed it will be 'tweeted and then deleted' in the presence of another member of staff.

Visitors must turn their mobile phones off when entering school and should be challenged if seen using a camera inappropriately or photographing children.

The use of cameras or mobile phones are prohibited in the toilets.

Communications Technologies and Social Media

A wide range of communications technologies has the potential to enhance learning and management. The acceptable use agreements outline how these systems should be used.

- The official school email service is used for communications between staff, and with parents/carers and students as it provides an effective audit trail. Communications are always professional in tone and content.
- Users are made aware that email communications may be monitored and what to do if they receive an email that makes them feel uncomfortable, is offensive, threatening or bullying in nature through the acceptable use policies.
- Governor communications take place through governor school e-mail accounts. Personal or sensitive information is not e-mailed but is kept on a secure drive on the school computer system.
- Personal email addresses, text messaging, public chat and social networking programmes are not be used for communications with parents/carers and children.
- The school X account (formally Twitter) is the responsibility of the headteacher and is monitored daily.
- Personal information is also not posted on the school website and parents are given the main office email address in order to contact staff. The web site is the responsibility of the headteacher and is monitored by governors.

- Guidance on personal use of social media and mobile devices is included in the staff, parent and pupil acceptable use policies including clear reporting mechanisms. Training is provided for staff and risks, reporting and issues around social networking forms part of the learning for pupils.
- Staff ensure that no reference is made in social media to pupils, parents or other staff and do not engage in online discussions on personal matters about any member of the school community
- Personal opinions are not attributed to the school
- Security settings on personal social media profiles are regularly checked to minimise risk
- Staff personal use of social media where it does not relate to the school is outside the scope of the policy but is should be made clear that the member of staff is not communicating on behalf of the school. If staff come across communications that might bring the school into disrepute in their personal communications, they should not get involved, refer the publisher to relevant complaints procedures and report the issue.
- Staff must never add pupils as 'friends' into their personal accounts (including past pupils under the age of 18).
- Staff are strongly advised not to add parents as 'friends' into their personal accounts
- Staff must not use social networking sites within lesson time (for personal use).
- Staff should only use social networking in a way that does not conflict with the current National Teacher Standards
- Inappropriate use by staff should be referred to the headteacher in the first instance and may lead to disciplinary action.

Comments posted by Parents/Carers

Parents and carers will be made aware of their responsibilities regarding their use of social networking. Methods of school communication include the prospectus, the website, newsletters, letters and verbal discussion. School policies and documents provide further information regarding appropriate channels of communication and means of resolving differences of opinion. Effective communication following principles of mutual respect is the best means of ensuring the best learning experiences for the child.

- Parents must not post pictures of pupils, other than their own children, on social networking sites where these photographs have been taken at a school event.
- Parents should make complaints through official school channels rather than posting them on social networking sites.
- Parents should not post malicious or fictitious comments on social networking sites about any member of the school community.

Dealing with incidents of online bullying/inappropriate use of social networking sites

The school's Anti-Bullying Policy sets out the processes and sanctions regarding any type of bullying by a child on the school roll.

In the case of inappropriate use of social networking by parents, the Chair of Governors on behalf of the Governing Body will contact the parent asking them to remove such comments and seek redress through the appropriate channels such as the Complaints Policy and will send a letter.

The Governing Body understands that, "There are circumstances in which police involvement is appropriate. These include where postings have a racist element or where violence is threatened or encouraged." Furthermore, "Laws of defamation and privacy still apply to the web and it is unlawful for statements to be written…which:

- expose (*an individual*) to hatred, ridicule or contempt
- cause (*an individual*) to be shunned or avoided
- lower (*an individual's*) standing in the estimation of right-thinking members of society or
- disparage (*an individual in their*) business, trade, office or profession." (National Association of Headteachers)

Copyright

The headteacher is responsible for making sure that software licence audit is regularly updated and making regular checks to ensure the number of software installations matches the licences held. Where there are insufficient licences this could breach the Copyright Act, which may lead to fines or unexpected additional license costs.

Data Protection

Personal Data is defined as any data that relates to a living individual who can be identified from the data. This includes opinion about the individual. Sensitive Personal Data about a person includes information about their racial or ethnic origin, political opinions, their religious beliefs or other beliefs of a similar nature, whether they are a member of a trade union and their physical or mental health or condition. Actions are currently being implemented in order to ensure compliance with the new GDPR (Government Data Protection Regulation) and this policy will be updated in line with this new legislation.

Personal data is recorded, processed, transferred and made available according to the GDPR and is:

- 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 and only transferred to others with adequate protection

Transfer of Data

Whenever possible secure online storage is used to ensure that documents do not need to be transferred to limit the risk. We ensure that data is stored in accordance with the requirements laid down by the Information Commissioner's Office and within the EU. This also applies to cloud storage used.

The school ensures that:

- It holds the minimum personal data necessary to enable it to perform its function and does not hold it for longer than necessary for the purposes it was collected for.
- The data held is accurate, up to date and inaccuracies are corrected as quickly as possible.
- All personal data is fairly obtained in accordance with our "Privacy Notice" and lawfully processed in accordance with the "Conditions for Processing" as outlined in the policy on the South Gloucestershire IMS Traded Services web site.
- Personal and sensitive data relating to pupils or staff is not e-mailed as this is not secure.

- Personal data including assessment data is transferred using secure file transfer.
- Where information does need to be transferred between devices then encrypted memory sticks are used.
- It has clear and understood arrangements for the security, storage and transfer of personal data
- It is registered as a Data Controller for the purposes of the General Data Protection Regulations (GDPR)
- There is a Senior Information Risk Officer (SIRO) and Information Asset Owner (IAOs) in place.
- Risk assessments are regularly carried out.
- Data subjects have a right to access their data and there are clear procedures for this.
- There are clear and understood policies and routines for the deletion and disposal of data.
- There is a policy for reporting, logging, managing and recovering from information risk incidents.
- There are clear Data Protection clauses in all contracts where personal data may be passed to third parties.
- Only cloud storage that meets the requirements laid down by the Information Commissioner's office is used to store personal data.
- The staff acceptable use policy clearly defines the data protection measures that staff should take and how data can be securely stored and deleted.

Staff ensure that they

- Take care to ensure safe keeping of personal data and minimise the risk or loss or misuse
- Use personal data only on secure password protected computers and devices and log off at the end of every session
- Transfer data using encryption and secure password protected devices

Where personal data is stored on removable media:

- The data is encrypted and password protected
- The device is password protected
- The device has approved virus and malware checking software
- The data is securely deleted from the device once finished with.

Reporting and Recording

There are clear reporting mechanisms in place for online safety incidents and all staff are regularly reminded of these and fully aware of their responsibilities to follow up any reported issues.
Staff should report online safety issues are reported to the headteacher. If these include allegations of bullying then the anti-bullying policy is followed. Issues which may impact on the well-being and safety of a child are reported directly to the Child Protection Lead and Child Protection procedures are followed. Issues impacting on staff or to the detriment of the school should be reported to the headteacher or to the Chair of Governors if the headteacher is absent or the accusation involves the headteacher.
Pupils are encouraged to report any incidents to an adult whether it relates to themselves or a friend. We encourage children to take responsibility for protecting each other.

Managing Incidents

In the event of suspicion of an infringement of policy then all the following steps should happen.

- More than one senior member of staff should be involved in investigating to protect possible future accusations.
- Use a computer that will not be used by young people, which could be taken off site by the police if required.

- Ensure staff have internet access to investigate but that sites and content are closely monitored and recorded.
- Record the URL of any site containing alleged misuse and the nature of the content causing concern. It may be useful to record and store screenshots of the content by printing them, signing them and attaching them to the record. Not with child abuse images.
- Once the investigation is complete the investigating group should identify the appropriate response in line with policies which may include internal procedures, involvement of LA or police.

Reporting to the Police

If the content being reviewed includes images of child abuse then monitoring should be stopped and the police informed immediately. Other incidents to be referred to the police are:

- incidents of 'grooming' behaviour
- the sending of obscene materials to a child
- adult material which potentially breaches the Obscene Publications Act
- criminally racist material
- promotion of terrorism or extremism
- other criminal conduct, activity or materials

In any of the above incidents, isolate the computer involved as any change to its stage may hamper a police investigation.
If issues could be a result of problems with infrastructure or may affect it then the technical support provider is informed immediately (for South Gloucestershire support 863838).

If access to an unsuitable site is reported then the Online Safety lead will alert the technical support team by ringing 863838 to ensure that this is blocked. Serious incidents are escalated to local authority staff for advice and guidance

Nick Pearce – Infrastructure, Technical and Filtering - 863838
Tina Wilson – Safeguarding and Child Protection - 868508

For incidents affecting school staff the Professionals Online Safety Helpline is contacted for advice if necessary on helpline@saferinternet.org.uk or 0844 381 4772.

Any reported incidents are logged in the online safety log and followed up in accordance with the relevant policy depending on the issue. The response is also logged and serious issues are followed up after an interval of time to ensure that they are fully resolved.

Where appropriate school newsletters and the website are used to provide guidance to staff following an incident in order to prevent further incidents happening.

There are defined sanctions in place for any breaches of the acceptable use policies.

Appendix i: Roles and Responsibilities

Role	Responsibility
Governors	Approve and review the effectiveness of the online safety policy and acceptable use policies Online safety governor works with the online safety leader to carry out regular monitoring of online safety incident logs, filtering, changes to filtering and then reports to governors.
Head teacher and Senior Leaders:	Duty of care to ensure the safety (and online safety) of the school community. The headteacher and at least one other member of SLT should know the procedure to be followed in the event of a serious online safety allegation being made against a member of staff. Ensure that all staff receive suitable CPD to carry out their Online safety roles. Ensure that there is a system in place for monitoring and support of those who carry out the internal online safety role. Inform the local authority about any serious Online safety issues including filtering Ensure that the school infrastructure / network is safe and secure and that policies and procedures approved within this policy are implemented.
Online safety Leader (in this school, this is the headteacher)	Lead the online safety working group and deals with day to day online safety issues Lead role in establishing / reviewing online safety policies / documents and checking links to other policies Ensure all staff are aware of the procedures to follow if there is an online safety incident Provide and/or broker relevant training and advice for all school staff Attend updates and liaise with the LA online safety staff and technical staff Receives reports of online safety incidents and keeps the incident log updated Meet with online safety governor to regularly to discuss issues, review the incident log and filtering / changes to filtering log Report regularly to SLT Develop an online safety teaching programme to deliver the statutory programme of study. Monitor online safety teaching to ensure this is being delivered and is having an impact on pupils' understanding.
Child Protection Safeguarding Lead	Have received training in online safety issues and know the potential for child protection and safeguarding issues to arise from sharing personal data, access to illegal // inappropriate materials, inappropriate online contact with strangers, potential or actual incidents of grooming and cyber-bullying.
Curriculum Leaders	Ensure online safety is appropriately reflected in teaching programmes where relevant e.g. anti-bullying, English publishing and copyright and is reflected in relevant policies.
Teaching and Support Staff	Ensure they have an up to date awareness of school online safety issues, policies and practices. Have read, understood and signed the Staff Acceptable Use Agreement (AUP) Act in accordance with the AUP and Online safety policy Report any suspected misuse or problem to the headteacher / online safety leader. In the event that the incident involves the headteacher report to the governor responsible for safeguarding. Only communicate with pupils / parents / carers professionally through official school systems Ensure online safety issues are embedded in the curriculum and other activities

	Ensure pupils follow the online safety rules Ensure that the school programme of study for online safety is delivered through their teaching Monitor ICT activity in lessons, extra-curricular and extended school activities Deliver the scheme of work for online safety and ensure children have a good understanding of what they are being taught. Monitor use of digital technologies (mobile devices and cameras etc.) in lessons and other school activities where their use if allowed and implement policies about their use. Ensure that students are guided to appropriate sites in pre-planned internet use, that they are aware of how to search more safely and that any unsuitable material that is accessed is dealt with according to school policy. Immediately report any issues in accordance with school policy.
Students / pupils	Use schools systems in accordance with the pupil acceptable use policy Practice age-appropriate safe searching in order to reduce access to unsafe material Understand how to report online safety issues and do this immediately when an issue arises Know and follow the policies on use of mobile devices and cameras including taking images. Understand the importance of using technologies safely outside school and know that the policy covers actions out of school that are related to their membership of the school Help their friends to keep safe by pointing out any risks and what they could do about them
Parents and carers	Read the school guidance about online safety in the newsletter and on the website and take appropriate action if required to keep their child safe. Endorse (by signature) the Pupil Acceptable Use Policy Ensure that their child / children follow appropriate acceptable use rules at home Discuss online safety issues with their child / children and monitor their home use of ICT systems (including mobile phones and games devices) and the internet Access the school website / online platform in accordance with the relevant school Acceptable Use Policy. Keep up to date with issues through school updates and attendance at events Ensure they follow the school policy on taking digital and video images at school events Ensure their children following rules on appropriate use of children's' own devices in school Report any online safety issues that could impact on safeguarding of any children or learning in school so that the school can put in place appropriate measures and use these to inform any changes to teaching
Technical Support Provider	Ensure the school's ICT infrastructure is secure and is not open to misuse or malicious attack Ensure that the school meets Online safety technical requirements of the LA Ensure users may only access the school network through an enforced password protection policy, where passwords are regularly changed Ensure that filtering is robust is blocking but does not inhibit learning and teaching Keep up to date with online safety technical information and update others as relevant

	Ensure use of the network is regularly monitored in order that any misuse / attempted misuse can be reported to the headteacher / online safety leader for investigation / action / sanction. Ensure monitoring software / systems are implemented and updated Ensure all security updates / patches are applied (including up to date anti-virus definitions, windows updates) and take action to prevent spyware and malware.
Community Users	Sign and follow the AUP before being provided with access to school systems.

Appendix ii: Pupil Agreement

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:

Appendix iii: Parent Agreement

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 that 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.

Appendix IV: Staff Agreement

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