NONSUCH PRIMARY SCHOOL

E-SAFETY POLICY

Date of Policy: March 2015
Date of Review: March 2018
Author: Josh Chamberlin

This e-safety policy has been developed in line with current practice and with reference to current national recommendations. This policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to e-safety or incidents that have taken place.

The school will monitor the impact of the policy using logs of reported incidents and responses to surveys/questionnaires from various stakeholders in the school community.

Contents

Scope of the Policy

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

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

Aims

Through this policy, we aim to:

- Protect and educate pupils and staff in their use of technology
- Ensure the school has appropriate procedures in place for intervening and supporting when incidents occur
- Ensure that all staff, parents, governors and children understand the school's approach to e-safety.

Expectations of the School Community

Governors

Governors are responsible for the approval of the E-Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the Governors receiving regular information about e-safety incidents and monitoring reports.

Headteacher (and Safeguarding Designated Person)

- Has a duty of care for ensuring the safety (including e-safety) of members of the school community. The Headteacher, as safeguarding designated person, and Assistant Headteacher 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.
- Is responsible for ensuring that the E-Safety Coordinator and other relevant staff receive suitable training to enable them to carry out their e-safety roles and to train other colleagues, as relevant.
- Will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal e-safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.

The Headteacher, as safeguarding designated person, should be trained in e-safety issues and be aware of the potential for serious child protection / safeguarding issues to arise from:

- sharing of personal data
- access to illegal / inappropriate materials
- inappropriate on-line contact with adults / stranger
- potential or actual incidents of grooming
- cyber-bullying

E-Safety and Computing Coordinator

- takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policies / 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 technical staff (Cygnet IT)
- receives reports of e-safety incidents and creates a log of incidents to inform future e-safety developments
- attends relevant governor meetings
- reports regularly to the Senior Leadership Team
    - that the school's technical infrastructure is secure and is not open to misuse or malicious attack
    - that the school meets required e-safety technical requirements and any Local Authority / other relevant body E-Safety Policy / Guidance that may apply
    - that users may only access the networks and devices in line with the acceptable use agreements

- that they keep 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 / internet / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the Headteacher

Teachers

- have an up to date awareness of e-safety matters and of the current school e-safety policy and practices
- have read, understood and signed the Staff Acceptable Use Agreement
- report any suspected misuse or problem to the Headteacher or e-safety coordinator for further action
- ensure all digital communications with pupils / parents / carers should be on a professional level and only carried out using official school systems
- ensure opportunities for teaching e-safety are embedded in all aspects of the curriculum and other activities
- ensure pupils understand and follow the e-safety and acceptable use policies
- pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- monitor the use of digital technologies, mobile devices, cameras etc. in lessons and other school activities (where allowed) and implement current policies with regard to these devices
- in lessons where internet use is pre-planned, ensure pupils are 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

Parents

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 behaviours. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.

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

- Curriculum activities
- Letters, newsletters, website,
- Parents meetings
- High profile events / campaigns e.g. Safer Internet Day
- Reference to the relevant web sites / publications

Children

- are responsible for using the school digital technology systems in accordance with the pupil acceptable use agreement that they sign annually
- 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 practices on the use of mobile devices and digital cameras. They should also know and understand practices relating to the taking / use of images and 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

Community Users

Community Users who access school systems as part of the wider school provision will be expected to sign an acceptable use agreement before being provided with access to school systems.

Education

Whilst regulation and technical solutions are very important, their use must be balanced by educating pupils to take a responsible approach. The education of pupils in 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 should be a focus in all areas of the curriculum and staff should reinforce e-safety messages across the curriculum. The e-safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways:

- A planned e-safety curriculum is provided as part of Computing and other lessons and is regularly revisited
- Key e-safety messages are reinforced as part of a planned programme of assemblies and pastoral activities
- Pupils are 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 are taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Pupils are helped to understand the need for the pupil Acceptable Use Agreement and encouraged to adopt safe and responsible use both within and outside school
- Staff act as good role models in their use of digital technologies, the internet and mobile devices
- In lessons where internet use is pre-planned, it is best practice that pupils are 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 search the internet, staff are vigilant in monitoring the content of the websites the young people visit.

It is accepted that from time to time, for good educational reasons, pupils may need to research topics (e.g. racism, drugs, and discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the technical staff (or other relevant designated person) can

temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need.

Training

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

- Regular opportunities for e-safety training advice are provided. An audit of the e-safety training needs of all staff is carried out regularly. It is expected that some staff will identify e-safety as a training need within the appraisal process.
- All new staff receive e-safety training as part of their induction programme, ensuring that they fully understand the school e-safety policy and Acceptable Use Agreements.
- The e-safety coordinator (or other nominated person) will receive regular updates through attendance at external training events (e.g. from the LA / other relevant organisations) and by reviewing guidance documents released by relevant organisations.
- This e-safety policy and its updates will be presented to and discussed by staff in staff meetings.
- The e-safety coordinator (or other nominated person) will provide advice / guidance / training to individuals as required.

Governors are invited to attend training as part of the school or local authority training provision.

Technical – infrastructure, filtering and monitoring

The school is 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.

- School technical systems are managed in ways that ensure that the school meets recommended technical requirements.
- There are regular reviews and audits of the safety and security of school technical systems.
- Servers, wireless systems and cabling are securely located and physical access restricted.
- All users have clearly defined access rights to school technical systems and devices.
- The headteacher is responsible for ensuring that software licences are up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations.
- Internet access is filtered for all users.
- School technical staff regularly monitor and record the activity of users on the school technical systems and users are made aware of this in the Acceptable Use Agreement.
- An appropriate system is in place for users to report any actual / potential technical incident / security breach to the relevant person.
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, mobile devices, etc. from accidental or malicious attempts which might threaten the security of the school systems and data. These are tested regularly. The school infrastructure and individual workstations are protected by up to date virus software.
- An agreed policy is in place for the provision of temporary access of “guests” (e.g. trainee teachers, supply teachers, visitors) onto the school systems.

- Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured.

Use of digital and video images

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, parents / carers and pupils need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for cyberbullying to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. It is common for employers to carry 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 e.g. on social networking sites.
- Parents / carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use in not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published / made publicly available on social networking sites, nor should parents / carers comment on any activities involving other pupils in the digital / video images.
- Staff and volunteers are allowed to take digital / video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be 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 is obtained in order that photographs of pupils can be published on the school website. Where there is no written permission, photographs of these children are not published.

Data Protection

The school must ensure that:

- It will hold the minimum personal data necessary to enable it to perform its function and it will not hold it for longer than necessary for the purposes it was collected for.
- Every effort will be made to ensure that data held is accurate, up to date and that inaccuracies are corrected without unnecessary delay.

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.

Communication

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	wed	rtain mes	cted staff	wed	wed	rtain mes	staff sion	wed
Mobile phones may be brought to school	✓					✓		
Use of mobile phones in lessons				✓				✓
Use of mobile phones in social time	✓							✓
Taking photos on mobile phones / cameras		✓				✓		
Use of other mobile devices e.g. tablets	✓						✓	
Use of personal email addresses in school, or on school network		✓						✓
Use of school email for personal emails				✓				✓
Use of messaging apps		✓						✓
Use of social media		✓						✓
Use of blogs (the school blogsite)	✓				✓			

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

- The school email service is regarded as safe and secure and is monitored. Users should be aware that email communications are monitored.
- Users must immediately report, to the nominated person – in accordance with the school policy, the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.
- Any digital communication between staff and pupils or parents / carers must be professional in tone and content. These communications should only take place on official (monitored) school systems. Personal email addresses, text messaging or social media must not be used for these communications.
- Whole class / group email addresses may be used at KS1, while pupils at KS2 will be provided with individual school email addresses for educational use. Pupils are taught about e-safety issues, such as the risks attached to the sharing of personal details. They are also taught strategies to deal with inappropriate communications and are reminded of the need to communicate appropriately when using digital technologies.
- Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff.

Social Media

School staff should ensure that:

- No reference should be made in social media to pupils, parents / carers or school staff
- They do not engage in online discussion on personal matters relating to members of the school community
- Personal opinions should not be attributed to the school or local authority
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

Inappropriate behaviour

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 usage as follows:

User Actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Users shall not visit Internet sites,	**Child sexual abuse images –The making, production or distribution of indecent images of children. Contrary to The Protection of Children Act 1978**					✓

make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	**Grooming, incitement, arrangement or facilitation of sexual acts against children Contrary to the Sexual Offences Act 2003.**					✓
	Possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character) Contrary to the Criminal Justice and Immigration Act 2008					✓
	criminally racist material in UK – to stir up religious hatred (or hatred on the grounds of sexual orientation) - contrary to the Public Order Act 1986					✓
	pornography				✓	
	promotion of any kind of discrimination				✓	
	threatening behaviour, including promotion of physical violence or mental harm				✓	
	any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute				✓	
Using school systems to run a private business					✓	
Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school / academy					✓	
Infringing copyright					✓	
Revealing or publicising confidential or proprietary information (e.g. financial / personal information, databases, computer / network access codes and passwords)					✓	
Creating or propagating computer viruses or other harmful files					✓	
Unfair usage (downloading / uploading large files that hinders others in their use of the internet)					✓	
On-line gaming (educational)				✓		
On-line gaming (non-educational)				✓		
On-line gambling				✓		
On-line shopping / commerce			✓			
File sharing			✓			
Use of social media			✓			
Use of messaging apps				✓		
Use of video broadcasting e.g. YouTube		✓				

Responding to incidents of misuse

This guidance is intended for use when staff need to manage incidents that involve the use of online services. It encourages a safe and secure approach to the management of the incident. Incidents might involve illegal or inappropriate activities (see "User Actions" above).

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.

Pupils

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

Staff

Incidents (Staff):	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).	✓	✓		✓				✓
Inappropriate personal use of the internet / social media / personal email	✓	✓				✓		
Unauthorised downloading or uploading of files	✓				✓	✓		
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	✓				✓	✓		
Careless use of personal data e.g. holding or transferring data in an insecure manner	✓					✓		
Deliberate actions to breach data protection or network security rules		✓			✓	✓		✓
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software		✓			✓	✓		✓
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature		✓	✓	✓			✓	✓
Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with pupils		✓	✓					✓
Actions which could compromise the staff member's professional standing		✓	✓					✓
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school		✓						✓
Using proxy sites or other means to subvert the school's filtering system	✓					✓	✓	
Accidentally accessing offensive or pornographic material and failing to report the incident		✓	✓					
Deliberately accessing or trying to access offensive or pornographic material				✓			✓	
Breaching copyright or licensing regulations		✓						✓
Continued infringements of the above, following previous warnings or sanctions		✓					✓	✓

Information and further guidance for parents:

We have done all that is possible to ensure children are protected through the use of a filtered service and a requirement that a member of staff always supervises internet access. Our children are taught to use the facility sensibly - the rules concerning internet use are regularly discussed in class and we

welcome your endorsement of these. We strongly recommended that parents consider and develop a similar set of rules for the use of the internet outside of school. You might also like to discuss as a family the issues surrounding the downloading of music, mobile phones, social networking sites such as YouTube, and the use of games consoles, within the home environment. You may find the following websites useful to help ensure that children stay safe.

Childnet International is a non-profit organisation working to help make the Internet a great and safe place for young people. These sites are all created by this organisation:

www.childnet-int.org http://www.kidsmart.org.uk http://www.chatdanger.com

You can find downloadable safety leaflets here:
http://www.childnet-int.org/downloads/parents-leaflet.pdf

http://www.childnet-int.org/downloads/musicLeaflet.pdf

http://www.childnet-int.org/downloads/ICRA-Bill-of-Rights.pdf

http://www.childnet-int.org/downloads/a2poster.pdf

Other useful sites include:

Safe Kids	http://www.safekids.com
Cyber Patrol	http://www.cyberpatrol.co.uk
Net Nanny	http://www.netnanny.com
CBBC	http://www.bbc.co.uk/cbbc/help/safesurfing (aimed at KS1)
Bullying Online	http://www.bullying.co.uk
Think U Know	http://www.thinkuknow.co.uk