Learn together, learn forever

Hazel Grove Primary School

e-Safety Policy

Date: March 2017

Review Date: March 2020

POLICY APPROVED BY GOVERNORS:
POLICY RATIFIED BY GOVERNORS:

SIGNED: CHAIR OF GOVERNORS

SIGNED: HEAD TEACHER

Contents

Policy Governance

Policy Working Group

Position	Name
School e-Safety Officer	David Edwards
Head teacher	Anna Roche
Governor	Mark Saxon

Schedule for Review

This e-safety policy was approved by the Governing Body	March 2017
The implementation of this e-safety policy will be monitored by the:	Headteacher e-safety Officer Governor
Monitoring will take place at regular intervals:	Once per annum
Governing Body will receive a report on the implementation of the e-safety policy generated by Computing Co-ordinators (which will include anonymous details of e-safety incidents) at regular intervals:	Once per annum
The E-Safety Policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to e-safety or incidents that have taken place. The next anticipated review date will be:	March 2018
Should serious e-safety incidents take place, the following external persons / agencies should be informed:	LA ICT Manager: Garry Wilson LA Safeguarding Officer: Julia Storey Police: PCSO Mark Turner

Scope of the Policy

This policy applies to all members of the school community (staff, pupils, volunteers, parents, carers and visitors): Anyone who has access to, and are users of, ICT systems and mobile technologies in school. The policy also covers use of school electronic equipment out of school and electronic equipment which contains data relating to the school.

Roles and Responsibilities

Governor: Mark Saxon

- Governors are responsible for the approval of the E-Safety Policy and for reviewing the effectiveness of the policy.

Headteacher and Senior Leaders: Anna Roche & Gerry Rose

- The Headteacher is responsible for ensuring the safety (including e-safety) of members of the school community;
- 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.

E-Safety Officer: David Edwards

- leads the e-safety committee and / or cross-school initiative on e-safety;
- 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;
- receives reports of e-safety incidents and creates a log of incidents to inform future e-safety developments;
- reports regularly to Senior Leadership Team.

Network Manager / Technical staff: Garry Holmes

At Hazel Grove Primary School, our ICT and Network infrastructure is managed by RM. It is their responsibility for ensuring:

- that the school's ICT infrastructure is secure and is not open to misuse or malicious attack;
- that the school meets the e-safety technical requirements outlined in any relevant Stockport Metropolitan Borough Council E-Safety Policy and guidance;
- that users may only access the school's networks through a properly enforced password protection policy.

Teaching and Support Staff

- ensure they have an up to date awareness of e-safety matters and of the current school e-safety policy and practices;
- reads, understands and signs the school Staff Acceptable Use Policy & Agreement;
- promptly reports any suspected misuse or problem to the e-safety *Officer / Head Teacher* for investigation/action/sanction;

Designated person for child protection/Child Protection Officer: Anna Roche

should be trained in e-safety issues and be aware of the potential for serious child Protection issues that arise through the use of technology from:

- sharing of personal data;
- access to illegal / inappropriate materials;
- inappropriate on-line contact with adults, including strangers;
- potential or actual incidents of grooming;
- cyber-bullying.

e-Safety Committee

Members of the e-Safety Committee (Digital Leaders, e-Safety Officer, E safety Ambassadors/Parents Focus group) will assist the e-Safety Officer with:

- the production, review and monitoring of the school e-Safety Policy (Schools will need to decide the membership of the e-Safety committee, which may include students/parents)

Pupils:

- are responsible for using the school ICT systems and mobile technologies in accordance with the Pupil Responsible Use Policy, which they will be expected to sign before being given access to school systems (nb. at KS1 it would be expected that parents/carers would sign on behalf of the pupils)
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so.

Parents/Carers

The school will take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website and information about national / local e-Safety campaigns and literature. Parents and carers will be responsible for:

- endorsing (by signature) the Student Responsible Use Policy;
- accessing the school ICT systems in accordance with the school Responsible Use Policy.

e-Safety Education and Training

Pupils

e-Safety education will be provided in the following ways:

- A planned e-Safety programme will be provided as part of Computing / PHSE / other lessons and will be regularly revisited – this will cover both the use of ICT and new technologies in and outside school;
- Key e-Safety messages will be reinforced as part of a planned programme of assemblies and tutorial / pastoral activities;
- Pupils will be taught in all lessons which use online content, to be critically aware that they need to validate the accuracy of information they access on-line.

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. It is expected that some staff will identify e-Safety as a training need within the performance management process.
- All new staff will receive e-Safety training as part of their induction programme, ensuring that they fully understand the school e-Safety Policy and Responsible Use Policies.

Communication devices and methods

The following table shows the school’s policy on the use of communication devices and methods.

Where it is indicated that the method or device is allowed at certain times, these are clearly outlined in the next table.

	Staff & other adults				**Students/Pupils**			
Communication method or device	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff & parent permission	Not allowed
Mobile phones may be brought to school	✓						✓	
Use of mobile phones in lessons				✓				✓
Use of mobile phones in social time	✓							✓
Taking photos on personal mobile phones or other camera devices		✓						✓
Use of personal hand held devices e.g. PDAs, PSPs				✓				✓
Use of personal email addresses in school, or on school network				✓				✓
Use of school email for personal emails		✓						✓
Use of chat rooms / facilities				✓				✓
Use of instant messaging		✓						✓
Use of social networking sites				✓				✓
Use of blogs		✓					✓	

	Circumstances when these may be allowed	
Communication method or device	**Staff & other adults**	**Pupils**
Mobile phones may be brought to school.	School mobile on trips/school field and personal mobiles in break time only in the staff room	Only where a parent has requested e.g. to check a child permitted to go home alone in Y5/6 has arrived safely if the parent is not home
Use of mobile phones in lessons.		
Use of mobile phones in social time.	e.g. during breaks or after school.	
Taking photos on personal mobile phones or other camera devices.	e.g. during the staff room for personal reasons or after school but never of children	
Use of personal hand held devices eg PDAs, PSPs.		
Use of personal email addresses in school, or on school network.	On personal mobile devices only in social time.	
Use of school email for personal emails.		
Use of chat rooms / facilities.		
Use of instant messaging.	e.g. during breaks or after school.	
Use of social networking sites.		
Use of blogs.	e.g. set up for use in school.	e.g. blogs on VLE set up by teacher

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 should not engage in these activities in school or outside school when using school equipment or systems, 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, materials, remarks, proposals or comments that contain or relate to:	Child sexual abuse images –The making, production or distribution of indecent images of children. Contrary to The Protection of Children Act 1978.					✓
	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				✓	

User Actions	Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
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.				✓	
Infringe 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 on school computer				✓	
Use of messaging apps				✓	
Use of video broadcasting e.g. Youtube			✓		

Incident Management

Incidents (students/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
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 handheld device	✓					
Unauthorised use of social networking/ instant messaging/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 student's/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 instant 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 filtering system		✓				✓
Accidentally accessing offensive or pornographic material and failing to report the incident	✓					
Deliberately accessing or trying to access offensive or pornography		✓			✓	
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act		✓			✓	

Incidents (staff and community users):	Refer to Headteacher for decision and potential further action	Refer to Police	Refer to technical support staff for action re filtering / security etc	Removal of network / internet access rights	Warning
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities)	✓				
Excessive or inappropriate personal use of the internet / social networking sites / instant messaging / 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 eg 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 instant 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 students / 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					

Further information and support

Further information for parents/carers:

CEOP: www.ceop.gov.uk
Think U Know: www.thinkuknow.co.uk
Childnet: www.childnet-int.org

Recommended child friendly search engines:

Ask Jeeves for kids:
www.askkids.com

CBBC Search:
www.bbc.co.uk/cbbc/search

National Education Network:
www.nen.gov.uk/tandl

Yahoo! Kids:
www.kids.yahoo.com

Kidsclick:
www.kidsclick.org

e-Safety information booklet:

https://shareweb.kent.gov.uk/Documents/childrens-social-services/protecting-children/E-Safety/e-safety-children.pdf

Appendix 1 – Home / School Responsible Use Agreement

Responsible Electronic Equipment Use Document.

The use of electronic equipment is schools is ever changing; at Hazel Grove Primary we currently use laptops, iPads, iPods, digital cameras, interactive whiteboards and the internet, with this list set to increase over time. This document contains the responsibilities of the children, and the school, which will help us work together to keep the children safe.

Child's Responsibility

Using the computers:

- I will only access the computer system with the login and password I have been given;
- I will not look at or delete other people's files, unless I have permission from the owner;
- I will not bring in data from outside school and use it on school equipment without permission from a teacher. This includes data from memory sticks, discs or the internet.

Using the Internet:

- I will ask permission from a teacher before using the internet, social media, internet chat or downloading any documents or apps in school;
- I will report any unpleasant material to my teacher immediately because this will help protect other pupils and myself;
- I understand that the school will check all the files I create and the internet sites I visit;
- I will not put any information into the internet without permission from my teacher;
- I will not at any time put my full name, home address or telephone number into any electronic equipment at school;
- I will not access any personal email accounts or social media at school.

School's Responsibility

- Children will be taught safe use of all electronic equipment and the internet;
- Firewalls and banned lists will be used to ensure any site which could be harmful or upsetting cannot be accessed through the internet.
- Children's work and use of the internet will be monitored and any inappropriate materials deleted.
- Unauthorised use of the school's computer system, or the system being used for criminal purposes or for storing text or imagery which is unauthorised or unlawful, will result in a ban from using the electronic equipment at school.

Please discuss the responsibilities with your child, read the consent forms, then cut off the bottom, sign and return to the school office

Parent’s Consent for Internet Access

I have read and understood the school Rules for Responsible Internet and Electronic Equipment Use. I have discussed these with my child. I understand that by signing this document, I give permission for my son / daughter to access the Internet and use electronic equipment at school.
I understand that the school will take all reasonable precautions to ensure pupils cannot access inappropriate materials. I understand that the school cannot be held responsible for the nature or content of materials accessed through the Internet, but every effort will be used to ensure their safety.
I agree that the school is not liable for any damages arising from the use of the Internet facilities.

Parent’s Consent for Web Publication of Work and Photographs

I agree that, if selected, my son / daughter’s work may be published on the School Web Site.

✂ Please read, cut off, sign and return ✂

Pupil (Print Name) ……………………………………………………..…. Class/Year ……………………
Date …………………

Parent’s Consent for Web Publication of Work and Photographs

I also agree that photographs that include my son / daughter may be published subject to the school rules that photographs will not clearly identify individuals and that full names will not be used.

✂ Please read, cut off, sign and return ✂

Pupil (Print Name) ……………………………………………………..…. Class/Year ……………………
Date …………………

Pupil’s Agreement: I have read and understood the rules for Responsible Internet Use and eSafety. I will use the computer systems and Internet in a responsible way as described in the eSafety document.

Parent/Carer’s agreement: By signing this slip I, and the child in my care, agree to all the responsibilities and consent to using the internet and having images published, as described in the eSafety Document dated March 2017.

Parent/Carer Signature	Pupil Signature	Date

Appendix 2 – Staff, Volunteer RUP

Staff and Volunteer User Responsible Use Policy Agreement

School Policy

This Responsible Use Policy (RUP) is intended to ensure:

- that staff and volunteers will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.

- that school ICT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.

- that staff and volunteers are protected from potential risk in their use of ICT in their everyday work.

Hazel Grove Primary School will try to ensure that staff and volunteers will have good access to ICT to enhance their work, to enhance learning opportunities for pupils learning and will, in return, expect staff and volunteers to agree to be responsible users.

Responsible 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. I recognise the value of the use of ICT for enhancing learning and will ensure that students/pupils receive opportunities to gain from the use of ICT. I will, where possible, educate the young people in my care in the safe use of ICT and embed e-Safety in my work with young people.

For my professional and personal safety:

- I understand that the school will monitor my use of the ICT systems, email and other digital communications.

- I understand that the rules set out in this agreement also apply to use of school ICT systems (eg laptops, email, etc) out of school.

- I understand that the school ICT systems are primarily intended for educational use and that I will not use the systems for personal or recreational use.

- I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password.

- I will immediately report any illegal, inappropriate or harmful material or incident I become aware of, to the appropriate person.

- I will be professional in my communications and actions when using school ICT systems:

- I will not access, copy, remove or otherwise alter any other user's files, without their express permission.

- I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.

- I will ensure that when I take and/or publish images of others I will do so with their permission and in accordance with the school's policy on the use of digital/video images. I will not use my personal equipment to record these images. Where these images are published (e.g. on the school website) it will not be possible to identify by name, or other personal information, those who are featured.

- I will only communicate with pupils and parents/carers using official school systems. Any such communication will be professional in tone and manner.

- I will not engage in any on-line activity that may compromise my professional responsibilities.

The school and the local authority have the responsibility to provide safe and secure access to technologies and ensure the smooth running of the school:

- When I use my personal hand held/external devices (PDAs/laptops/mobile phones/USB devices etc) in school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment. I will also follow any additional rules in line with the School's E-Safety Policy set by the school about such use.

- 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 will not try to 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 try to use any programmes or software that might allow me to bypass the filtering/security systems in place to prevent access to such materials.

- I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings, unless this is allowed in school policies.

- I will not disable or cause any damage to school equipment, or the equipment belonging to others.

- I will only transport, hold, disclose or share personal information about myself or others, as outlined in the School/Local Authority Personal Data Policy (or other relevant school policy). Where personal data is transferred outside the secure school network, it must be encrypted.

- I understand that data protection policy requires that any staff or pupil data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by school policy to disclose such information to an appropriate authority.

- I will immediately report any damage or faults involving equipment or software, however this may have happened.

When using the internet in my professional capacity or for school sanctioned personal use:

- I will ensure that I have permission to use the original work of others in my own work.

- Where work is protected by copyright, I will not download or distribute copies (including music and videos).

Staff and Volunteer Responsible Use Agreement Form

This form relates to the student/pupil Responsible Use Policy (RUP), to which it is attached.

I understand that I am responsible for my actions in and out of school:

- I understand that this Responsible Use Policy applies not only to my work and use of school ICT equipment in school, but also applies to my use of school ICT systems and equipment out of school and my use of personal equipment in school or in situations related to my employment by the school.

- I understand that if I fail to comply with this Responsible Use Policy Agreement, I could be subject to disciplinary action. This could include a warning, a suspension, referral to Governors and/or the Local Authority and in the event of illegal activities the involvement of the police

    - **I have read and understood the School's E-Safety Policy**

I have read and understand the above and agree to use the school ICT systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) within these guidelines.

Name	
Position	
Signed	
Date	

Appendix 3 – Use of Images Consent Form

Use of Digital / Video Images

The use of digital/video images plays an important part in learning activities. Pupils and members of staff may be using digital or video cameras to record evidence of activities in lessons and out of school. These images may then be used in presentations in subsequent lessons.

Images may also be used to celebrate success through their publication in newsletters, on the school website and occasionally in the public media,
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 that 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	
Pupil Name	

As the parent / carer of the above 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	