Wheatfield Primary School

'Growing and Learning Together'

E Safety Policy

(Statutory Policy Document)
Issue No 3
April 2018

Approved by Head Teacher:	24 April 2018
Approved by Governors:	10 May 2018
Review Date:	May 2021

Wheatfield Primary School
Wheatfield Drive
Bradley Stoke
Bristol BS32 9DB

Tel: 01454 868610
Email: office@wheatfieldprimary.com
Website: www.wheatfieldprimary.com

CONTENTS

CHANGE RECORDS SHEET

Issue No.	Date	Summary of Change	Amended by
1	May 2014	Original policy document.	Sam O'Regan
2	November 2015	Document reviewed; all changes are highlighted in the left hand margin.	Sam O'Regan
3	April 2018	Document reviewed. All references to the old Data Protection Act are changed to the EU's GDPR. All changes are highlighted in the left hand margin.	Denise Hickson

SUMMARY

This policy should be read in conjunction with all other school policies. If you require further details of this policy then please refer to the Head Teacher or Deputy Head Teacher.

This policy will be reviewed every three years or updated as and when changes require an immediate update to policy.

ABBREVIATIONS

The following abbreviations are used in the policy:

CPD Continuing Professional Development

EUEU European Union

GDPR General Data Protection Regulation

ICT Information and Communications Technology

LA Local Authority

SWGfL South West Grid for Learning

MAIN DOCUMENT

1 RATIONALE

The internet and other technologies have the potential to offer many positive benefits to young pupils. As with everything, this is not without risk. We want pupils to be able to fully exploit the benefits offered by ICT, while doing so in a safe manner. Online messaging, social networking and mobile technology effectively mean that children can always be "online". Their social lives, and therefore their emotional development, are bound up in the use of these technologies.

The purpose of this policy is to ensure that the school community is kept aware of the risks, as well as the benefits of technology and how to manage these risks and keep themselves and others safe. It details the measures that the school have put in place to support this.

2 SCOPE OF THE POLICY

This policy applies to all members of the school community (including staff, students, volunteers, parents/carers, visitors and community users) who have access to and are users of school ICT systems. It applies to systems in school and out of school where activities have been set by the school or are using school online systems.

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

3 ROLES AND RESPONSIBILITIES

The following roles and responsibilities have been allocated and agreed across the school:

Role	Responsibility
Governors	Approve and review the effectiveness of the E-Safety Policy and Acceptable Use Policy. E-Safety Governor works with the ICT subject leader to carry out regular monitoring of e-safety incident logs, filtering, changes to filtering and then reports to Governors.
Head teacher and Senior Leaders	Ensure that all staff received suitable CPD to carry out their e-safety roles and sufficient resource is allocated. Ensure that there is a system in place for monitoring e-safety. Follow correct procedure in the event of a serious e-safety allegation being made against a member of staff. Inform the local authority about any serious e-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.
ICT Subject Leader	Deal with day to day e-safety issues. Lead role in establishing/reviewing e-safety policies and documents. Ensure all staff are aware of the procedures outlined in policies.

	Provide and/or brokering raining and advice for staff. Attend updates with the LA e-safety staff. Liaise with technical staff. Deal with and log e-safety incidents including changes to filtering. Meet with E-Safety Governor regularly to monitor e-safety developments. Report regularly to Senior Leadership Team.
Curriculum Leaders	Ensure e-safety is reflected in teaching programmes where relevant, e.g. anti-bullying, English publishing and copyright and is reflected in relevant policies.
Teaching and Support Staff	Participate in any training and awareness raising sessions. Have read, understood and signed the Staff Acceptable Use Agreement. Act in accordance with the Acceptable Use Policy and E-Safety Policy. Report ay suspected misuse or problem to the ICT Co-Ordinator. Monitor ICT activity in lessons, extra-curricular and extended school activities.
Students / Pupils	Participate in e-safety activities, follow the Acceptable Use Policy and report any suspected misuse. Understand that the E-Safety Policy covers actions out of school that are related to their membership of the school.
Parents and Carers	Endorse (by signature) the Student / Pupil Acceptable Use Policy. Ensure that their child/children follow acceptable use rules at home. Discuss e-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 in accordance with the relevant school Acceptable Use Policy. Keep up to date with issues through school updates and attendance at events.
Technical Support Provider	Ensure the school's ICT infrastructure is secure in accordance with Becta guidelines and is not open to misuse or malicious attack. Ensure users may only access the school network through an enforced password protection policy, where passwords are regularly hanged for those who access children's data. Inform the Head teacher of issues relating to the filtering applied by the SWGfL. Keep up to date with e-safety technical information and update others as relevant. Ensure use of the network is regularly monitored in order than ay misuse/attempted misuse can be reported to the E-Safety Co-Ordinator 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 that reasonable attempts are made to prevent spyware and malware.
Community Users	Sign and follow the AUP before being provided with access to school systems.

4 EDUCATION OF PUPILS AND THE CURRICULUM

Whilst regulation and technical solutions are important, their use must be balanced by educating learners to take a responsible approach. The education of students in e-safety is an essential part of our 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.

We have an age-related e-safety curriculum that is used to promote e-safety through teaching pupils how to stay safe, how to protect themselves from harm, understand how to manage risk, and how to take responsibility for their own and others safety and how to be responsible users of technology.

E-safety is embedded in all relevant areas of the curriculum including research in History/Geography, publishing in English, social skills in PSHE, data handling in Mathematics and core skills in ICT.

The e-safety scheme of work identifies for each year group progression statements, learning outcomes, processes, skills, vocabulary, suggested software and web links, sample activities and assessment activities. Key e-safety messages are also reinforced through assemblies and through our annual E-Safety Week.

The Acceptable Use agreement is discussed with pupils in every class and all classes discuss their rules for e-safety which are displayed in all classrooms. Pupils are given age appropriate support to search safely and to evaluate the content that they access online. 'Hector' is installed on all laptops within school and children are reminded in every year group to use Hector if they come across any unsuitable material online. Staff are vigilant in monitoring the content of websites pupils visit and encourage pupils to use specific search terms, to reduce the likelihood of coming across unsuitable material.

Pupils are taught 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.

Staff use their teacher laptop to share with pupils, how to deal with issues outside school, where there may be no filtering.

Reference is also made to e-safety in the Home-School Acceptable Use policy.

5 EDUCATION OF PARENTS / CARERS

Parents and carers may have only a limited understanding of e-safety issues and may be unaware of risks and what to do about them. They have a critical role to play in supporting their children with managing e-safety risks at home, reinforcing key messages about e-safety and regulating their home experiences. The school supports parents to do this by:

- Providing clear acceptable use policy guidance.

- Providing a regular awareness raising e-safety session for parents
- Inviting parents to attend activities such as e-safety week and e-safety assemblies
- Providing a webpage on our website teaching parents and children about safe use of technologies.

6 EDUCATION AND TRAINING - STAFF AND GOVERNORS

There is a planned programme of e-safety training for all staff and governors to ensure they understand their responsibilities, as outlined in this, and the acceptable use policies.

- An audit of the e-safety training needs of all staff is carried out annually and this is used to plan professional development.
- All new staff receive e-safety training as part of their induction programme.
- The Head teacher and ICT subject leader receives regular updates through attendance at SWGfL and LA training sessions and through regular e-safety updates from the local authority.
- The E-Safety and Acceptable Use Policies are discussed in staff meetings.
- Staff act as good role models for students in their own use of ICT.
- Governors are included in e-safety awareness sessions and training. The e-safety governor attends local authority and SWGfL updates and disseminates these to the wider governing body.

7 USE OF DIGITAL AND VIDEO IMAGES

Digital imaging technologies create significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff and pupils need to be aware of the risks associated with sharing images and with posting digital images on the internet. The school informs and educates users about these risks and implements policies to reduce the likelihood of the potential for harm. Staff and pupils follow the clear guidance in the acceptable use policy concerning the sharing, distribution and publication of images.

Parents sign a consent form which allows photographs of their child to be used for publications, on twitter and on the web site. Photographs are carefully chosen and any published photographs or videos of pupils will not be used alongside full names.

8 GDPRGDPR

The school fully complies with the EUU's Data Protection Regulation. Staff ensure that they keep personal data safe, and use personal data only on secure password protected computers/devices, ensuring they are properly logged off at the end of a session using personal data. Staff ensure that any personal data on portable devices is encrypted and secure password protected and they delete personal data from portable devices once they have finished with it.

9 PASSWORDS

All users of ICT systems log in with an individual user name to ensure that all only have access to the data they have a right to access. Pupils are aware of the importance of keeping their passwords secret. Once children reach KS2, they are encouraged to change their own password from the one given to them in KS1. Staff are aware of the need to change their own network passwords on a regular basis, just as they do with

their South Gloucestershire email account. Staff passwords for the school Twitter account, @wheatfieldpri and the school website will be changed annually.

10 FILTERING

Filtering is provided through SWGfL internet service. Any changes to filtering are requested and managed through the South Gloucestershire IT helpdesk for all South Gloucestershire schools.

11 USE OF PERSONAL EQUIPMENT IN SCHOOL

Staff have use of school cameras and video recording devices, so use of personal device images and video is not necessary or allowed. However, the school acknowledges that personal mobile devices (such as smart phones with cameras) offer an opportunity for information sharing with parents via security protected Twitter accounts. Staff may therefore use cameras on phones to facilitate this, but must immediately delete images stored on the phone after uploading them.

Staff personal mobile phones should not be used to store contact details of parents and pupils. There is a school mobile phone which should be used for school visits.

12 COMMUNICATIONS TECHNOLOGIES

A wide range of communication technologies have the potential to enhance learning. The official school email service is used for communications between staff, and with parents/carers and students, as it is regarded as safe and secure, provides an effective audit trail and is monitored. The following table shows how the school allows communication technologies to be used.

	Staff & other adults				Students / Pupils			
Communication Technologies	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission	Not allowed
Mobile phones may be brought to school	X						X	
Use of mobile phones in lessons		X						X
Use of mobile phones in social time	X							
Taking photos on mobile phones or other camera devices			X					X
Use of personal gaming devices				X			X	
Use of personal email addresses in school, or on school network				X				X
Use of school email for personal emails				X				X
Use of open chat rooms / facilities		X	X					X
Use of school limited chat facilities	X				X			
Use of public instant messaging				X				X

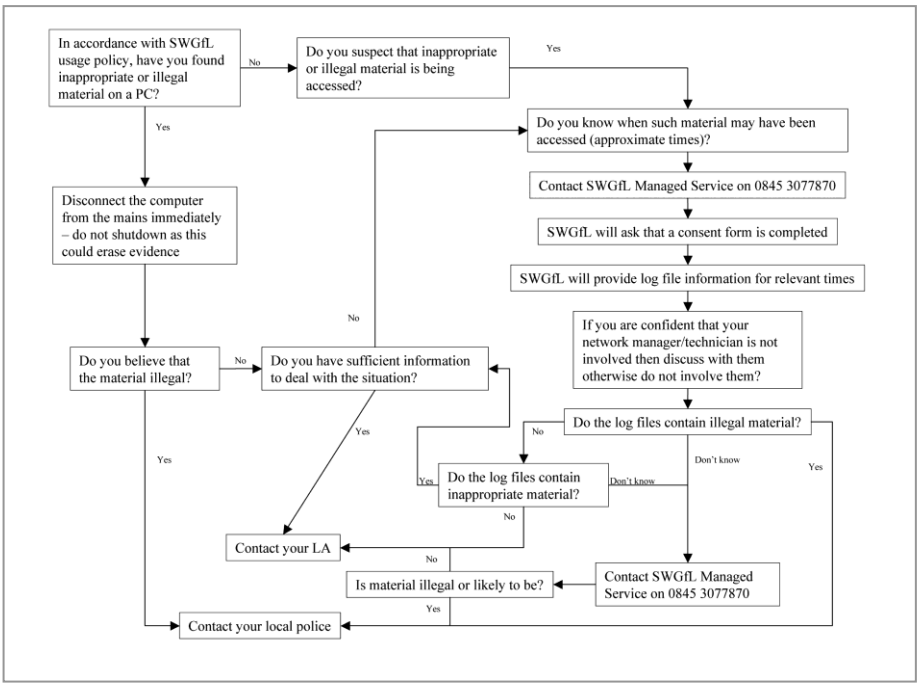
	Staff & other adults				Students / Pupils			
Communication Technologies	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission	Not allowed
Use of instant messaging across the school community	X					X		
Use of social networking sites			X					X
Use of moderated social networking sites only across the school community			X					X
Use of blogs	X						X	
Use of moderated blogs only across the school community	X						X	

13 REPORTING AND DEALING WITH INCIDENTS

There are activities that are inappropriate in a school context and users should not engage in these activities in school or outside school when using school systems. These are detailed in Appendix A.

We expect all members of the school community to be responsible users of ICT, who understand and follow this policy. However, there may be times when infringements of the policy take place, through careless, irresponsible or, very rarely, deliberate misuse. School-based online reporting processes are clearly in place and understood by the whole school. They are detailed in the Acceptable Use Agreements and are summarised as follows:

- Pupils report any issue to their teacher or other adult
- Staff must immediately report any issue to the ICT subject leaders, using the form which is available on the staff section of our website, and, in the case of possible child protection issues, to the head teacher who is responsible for child protection
- Any issues that cannot be resolved by the teacher are escalated to involve the head teacher
- ICT subject leader must report any issues to do with filtering to the local authority help desk. E-safety issues can also be escalated and should be reported to the following local authority staff.
    - Vicki Green – Safeguarding
    - Andreas Burt – Technical
    - Jo Briscombe – Teaching and Learning
- If any misuse appears to involve illegal activity the SWGfL flow chart below is consulted and followed, in particular the sections on reporting the incident to the police and the preservation of evidence.



If members of staff suspect that any misuse might have taken place it is essential that correct procedures are used to investigate, preserve evidence and protect those carrying out the investigation. In such event the SWGfL "Procedure for Reviewing Internet Sites for Suspected Harassment and Distress" will be followed. This guidance recommends that more than one member of staff is involved in the investigation which should be carried out on a "clean" designated computer. The school is more likely to encounter incidents that involve inappropriate rather than illegal misuse.

APPENDIX A UNSUITABLE / INAPPROPRIATE ACTIVITIES

The school believes that the activities referred to below are inappropriate school and that users should not engage in these activities in school or outside school when using school equipment or systems.

User Actions		Acceptable	Acceptable at certain times	Acceptable for nominated	Unacceptable	Unacceptable and illegal
Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	Child sexual abuse images					✓
	Promotion or conduct of illegal acts, e.g. Under child protection, obscenity, computer misuse and fraud legislation					✓
	Adult material that potentially breaches the Obscene Publications Act in the UK.					✓
	Criminally racist material in UK.					✓
	Pornography.				✓	
	Promotion of any kind of discrimination.				✓	
	Promotion of racial or religious hatred.				✓	
	Threatening behaviour, including promotion of physical violence or mental harm.				✓	
	Any other information which may be offensive to colleagues breaches the integrity of the ethos of the school or brings the school into disrepute.				✓	
Using school systems to run a private business.					✓	
Use systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by SWGfL and / or the school.					✓	
Uploading, downloading or transmitting commercial software or any copyrighted materials belonging to third parties, without the necessary licensing permissions.					✓	
Revealing or publicising confidential or proprietary information (e.g. financial / personal, databases, computer / network access codes and passwords).					✓	
Creating or propagating computer viruses or other harmful files.					✓	
Carrying out sustained or instantaneous high volume network traffic (downloading / uploading files) that causes network congestion and hinders others in their use of the internet.					✓	

User Actions	Acceptable	Acceptable at certain times	Acceptable for nominated	Unacceptable	Unacceptable and illegal
On-line gaming (educational).		✓			
On-line gaming (non educational).			✓		
On-line gambling.				✓	
On-line shopping / commerce.			✓		
File sharing.				✓	
Recreational use of social networking during directed time (staff)					
Use of social networking sites apart from Merlin e.g. Bebo, Facebook for older users.				✓	
Use of video broadcasting e.g. Youtube.			✓		