



E-Safety Core Policy



Written by The Staff of Durand

February 2015

Agreed March 2015

Durand Primary School

E-Safety Core Policy

E-Safety encompasses the use of new technologies, internet and electronic communications such as: mobile phones, collaboration tools and personal publishing.

The school's e-safety policy will operate in conjunction with other policies and guidance including:

- MCC Safeguarding Policy
- Behaviour and Discipline Policy
- Anti-Bullying Policy
- Child Protection
- PSE Policy
- Curriculum Policies
- Data Protection and Security guidelines

E-Safety depends on effective practice at a number of levels:

- Responsible ICT use by all staff and students; encouraged by education and made explicit through published policies and clear guidance.
- To teach children to use the Internet safely under supervision, and then help them to develop the skills and understanding they need to manage their own risk as they use the Internet independently.
- Sound implementation of e-safety policy in both administration and curriculum.
- Safe and secure broadband including the effective management of filtering.
- A member of staff being responsible for the implementation and monitoring of this e-safety policy.
- All staff should be vigilant in both their use of technology and the monitoring of pupil use in the context of their safeguarding responsibilities.

Introduction

The purpose of this policy is to:

- Through consultation with pupils establish the ground rules we have in Durand Primary for using the Internet and electronic communications such as mobile phones, tablets, collaboration tools and personal publishing. It highlights the need to educate pupils about the benefits and risks of using technology and provides safeguards and awareness for users to enable them to control their online experience.
- Describe how these fit into the wider context of our discipline and PSE policies.
- Demonstrate the methods used to protect children from sites containing pornography, racist or politically extreme views, bullying and violence
- Understand that accessing inappropriate sites accidentally is not something to feel guilty about and that any such incident should be shown to staff immediately and dealt with using the schools agreed protocol.

Teaching and Learning

- The Internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide students with quality Internet access as part of their learning experience.

- Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils.
- The school Internet access is designed expressly for teacher reference and for pupil use and includes filtering.
- Pupils are taught what Internet use is acceptable and what is not and are given clear objectives for Internet use.
- Pupils are educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.
- The school ensures that the use of Internet derived materials by staff and pupils complies with copyright law.
- Pupils are taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
- *Hwb+ is a learning platform for educators and learners to share resources, knowledge and experience across the whole of Wales.*
- Children are taught the benefits of mobile technologies and how to use them safely.
- The school endeavours to create a consistent message with parents for all pupils and this in turn should aid establishment and future development of the schools' e-Safety rules.
- However, staff are aware that some pupils may require additional support or teaching including adapted resources, reminders, prompts and further explanation to reinforce their existing knowledge and understanding of e-Safety issues.

Managing Internet Access

- School ICT systems capacity and security is reviewed regularly.
- Virus protection is updated regularly.
- Pupils are not allowed to bring mobile phones to school.

E-mail

- Pupils may only use approved e-mail accounts.
- Pupils must immediately show a member of staff or trusted adult if they receive offensive e-mail.
- Pupils must not send offensive or inappropriate e-mails.
- Pupils must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone.
- E-mail sent to an external organisation must be authorised before sending, in the same way as a letter written on school headed paper.
- The school reserves the right to access pupil email accounts if a concern is raised regarding inappropriate content.

School Web site or Blog

- The contact details on the Web site should be the school address, e-mail and telephone number. Staff or pupils' personal information is not published.
- The head teacher has overall editorial responsibility and ensures that content is accurate and appropriate.
- To ensure the safeguarding of all pupils, photographs or pupil names are never published together. It is encouraged not to publish individual photographs. Only first names or pupil initials are used.
- Written permission from parents or carers must be obtained before photographs or videos of pupils are published on the school Web site (*see Appendix 1 for sample permission form*).
- Pupil's work will only be published with the permission of the pupil and parents.

Social Networking and Personal Publishing

- Children are taught to use appropriate social networking sites safely for educational purposes.
- Children are discouraged from using social networking sites that are not age appropriate.
- 'Chat Rooms' are blocked.
- Pupils are told never to give out personal details of any kind which may identify them.
- Pupils must not attempt to gain access to another person / pupils account.
- Pupils are taught not to share their passwords.

Cyber Bullying

Cyber Bullying is a form of bullying through the use of ICT. An effective whole school approach to the prevention of cyber bullying should include:

- An agreed whole school understanding of cyber bullying;
- Talking about cyber bullying;
- Encouraging children to report cyber bullying;
- Promoting the positive and appropriate use of technology;
- Regularly monitoring the impact of this policy and the teaching and learning of e-safety.

Responding to incidents of cyber bullying should be dealt with using the schools existing behaviour and bullying prevention policies and procedures. *(See appendix 2 for further guidance).*

If cyberbullying takes place outside of school and has a negative impact on the orderly running of the school and/or might pose a threat to another pupil during school time or a member of staff then the head teacher **may take reasonable** steps to mediate between parties.

Managing Filtering

- If staff or pupils discover an unsuitable site, it must be reported and shown immediately to a member of school staff in accordance with the school's protocol.
- A senior staff member ensures that regular checks are made to ensure that the filtering methods are appropriate and effective.

Managing Video Conferencing (Skype)

- Video conferencing uses the educational broadband network to ensure quality of service and security rather than the Internet.
- Pupils must ask permission from the supervising teacher before making or answering a video conference call.
- Video conferencing is appropriately supervised for the pupils' age.

Managing Emerging Technologies

- Emerging technologies are examined for educational benefit and a risk assessment is carried out before use in school is allowed.

Protecting Personal Data

- Personal data is recorded, processed, transferred and made available according to the Data Protection Act 1998.

Policy Decisions

Acceptable Use

- All staff and pupils read and sign the ICT 'Acceptable Use Policy' before using any school ICT resources (*see Appendix 3 and 4 for examples*).
- The school keeps the signed up to date record of all staff and pupils who have agreed to the Acceptable Use Policy.
- Pupils are asked to re-sign an AUP in year 3.

Assessing risks

- The school takes all reasonable precautions to ensure that user's access only appropriate material by using Monmouthshire's filtering system.
- The school audits ICT provision on an annual basis to establish if the e-safety policy is adequate and that its implementation is effective.

Handling e-safety complaints

- Serious complaints of e-safety misuse are recorded by the member of staff that receives the complaint and reported to the Head.
- Any complaint about staff misuse is referred immediately to the head teacher.
- Any complaint about the Head is referred to the Governing body following the school's Complaints Policy.
- Complaints of a child protection nature are dealt with in accordance with the school's child protection procedures, MCC Safeguarding Policy and the All Wales Child Protection Procedures
- The schools' Complaints Policy is available on the school website.

Communications

Introducing the e-safety policy to pupils

- E-safety rules are posted in all rooms/classrooms and discussed with the pupils every year (*see Appendix 7 for example*).
- As part of the schools e-safety work all pupils and their parents are informed of the child exploitation and online protection centre: www.thinkuknow.co.uk

Staff and the e-Safety policy

- All staff have copies of the school's e-Safety Policy and know its importance.
- Staff are aware of their responsibility to safeguard all pupils in their use of technology in learning.
- The staff AUP is regularly discussed and agreed at staff meetings

Enlisting parents' support

- Parents' attention is drawn to the school's e-Safety Policy in newsletters, the school brochure and on the school Web site.
- The pupil AUP is sent home during reception and year 3 for parents to discuss with their children, sign and return.

- Parents are requested to follow the schools complaints procedures and not use social media.

Working with the Police

- The school works in partnership with the Schools Community Police Officer (SCPO) as part of the schools e-safety work.
- Some forms of cyber bullying behaviour may involve criminal offences and in these cases the school will contact the SCPO in line with the schools bullying prevention policy.

This policy will be review annually by the governors and staff or in light of new guidance.

Headteacher:

Chair of Governors:

Date:

Appendix 1



STILL, VIDEO AND ELECTRONIC PHOTOGRAPHY

There are many occasions during a pupil's time in school when both school and family might wish to record events for posterity e.g.:

- Concerts, musicals, festivals, sporting events.
- School, County and National honours.
- Visits from the media profiling high status events, and visiting dignitaries.
- Updating the school prospectus and website.
- Celebrating good work and achievement.
- Photography by pupils for Information Communication Technology (ICT) use or extra-curricular activities such as film clubs.

It is our passionate belief that the benefits for a child's self-esteem & confidence of having their photograph displayed in school or on the school website outweigh any risks when they are used correctly.

All photographs & videos taken in school comply with clear guidelines laid down by the Department for Education, Welsh Government and other professional bodies. No detailed personal information will accompany a visual image.

Nevertheless, in some circumstances we understand that there might be good reasons why parents/carers would not wish their child to be photographed or videoed. By signing below, you are giving approval for the school to photograph memorable moments in the life of the school which may include your child.

Parental consent will remain valid whilst a child is a pupil at the school and after they have left. However parents/carers have the right to withdraw that consent.

Name of Child _____

Class: _____

Please tick as appropriate:

		(✓)
A	I give permission for the school to take & use photographs & videos of my child in accordance with national guidelines for schools: <ul style="list-style-type: none"> ○ at school and on school arranged visits; 	
B	I give permission for the school to take & use photographs & videos of my child in accordance with national guidelines for schools: <ul style="list-style-type: none"> ○ for use in school documents, on the school website and in the press 	
C	I give permission for photographs & videos of my child to be used in accordance with national guidelines for schools by school approved third parties e.g. Gwent Music, Monmouthshire County Council: <ul style="list-style-type: none"> ○ for use by approved third party on websites and in promotional documentation 	

Please note:

If you feel that you are unable to select any of the above options please discuss with a member of school staff.

Signed (Parent/Carer):Date:.....

Appendix 2

Advice for Staff when inappropriate ICT use has been reported (including cyber bullying)

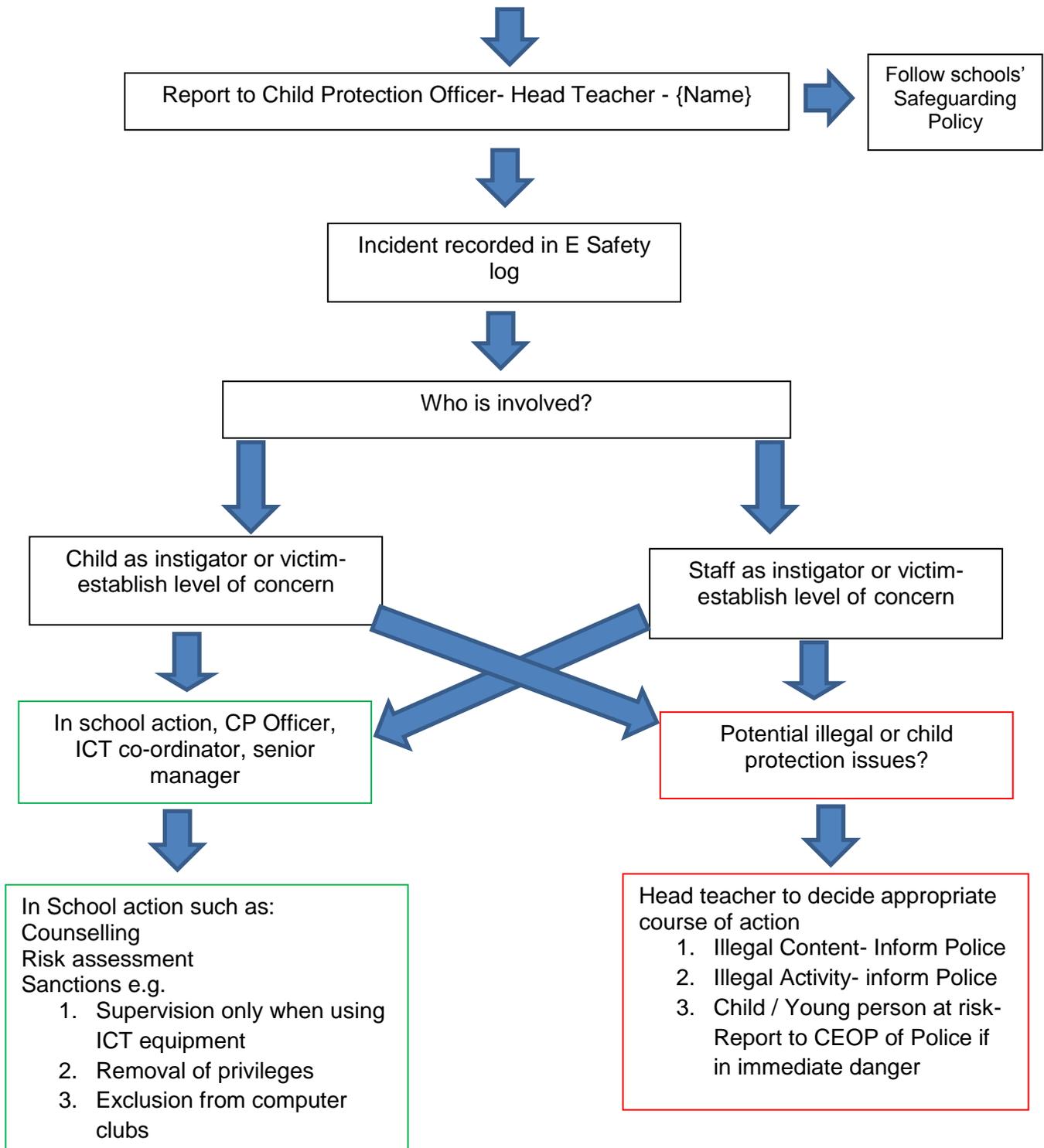
As part of the schools' e-safety work pupils are encouraged to show or tell a member of staff when inappropriate materials or behaviour have been witnessed.

Q. Can the incident be dealt with effectively by the member of staff? Yes / No

- If no then complete an e-safety log (below) attach any evidence and submit to the Head.
- If the incident relates to cyber bullying or child protection then please refer to the suggested 'cause for concern' flow chart.
- Advise the pupil how they may protect themselves in the future.

DO NOT REQUEST THAT A PUPIL FORWARDS THE MESSAGE / PHOTO TO YOUR DEVICE

E-Safety Log (Example)		
Date & Time:	Reported to:	Pupils Name:
Evidence attached Y/N		
Further information:		
Details of action taken:		
Signed (by head teacher):		Date:
Does SRS need to be informed? Y/N		



Foundation Phase ICT Acceptable Use Policy

I will read and follow the rules in the Acceptable Use Policy.

I understand that this Acceptable Use Policy is regularly reviewed and that there are consequences if I do not follow it.

- I will always use what I have learned to keep myself safe.
- I will tell a teacher if something makes me unhappy.
- I will use school computers for school work.
- I will only go on websites that my teacher tells me to.
- I will tell my teacher straight away if I go on a website by mistake.
- I will look after school ICT equipment and tell a teacher straight away something is broken or not working properly.
- I will only use the username and password I have been given and I will keep them safe.
- I will check with my teacher before printing.

I agree that any of my school work may appear on the school web site.

I understand that I must follow these rules to keep myself safe.

Signed on behalf of child, Parent/Carer's Signature:

Pupil Name:

Date:

Key Stage 2 ICT Acceptable Use Policy

I will read and follow the rules in the Acceptable Use Policy.



I understand that this Acceptable Use Policy is regularly reviewed and that there are consequences if I do not follow it.

- I will always use what I have learned about e-safety to keep myself safe and will tell a teacher if something makes me worried or unhappy.
- I will only use school e-Learning equipment for my school work and not to upset or bully other people or create a bad impression of my school.
- I will take responsibility for my own use of all e-Learning equipment and will use it safely, responsibly and legally.
- I will not go on any unsuitable or illegal web sites on purpose e.g. rude images, violence and racism. If I go on any by mistake I will tell a teacher straight away.
- I will tell a teacher if I can see a website that is inappropriate or receive any unwanted messages.
- I will look after school ICT equipment and report any damage to a teacher straight away.
- I will not try to get past any security measures in place to protect the school network.
- I will only use the usernames and passwords I have been given and I will keep them secret.
- I will save only school work on the school network and will check with my teacher before printing.
- I will not take photographs or movies of other staff and pupils other instructed by the teacher.
- I will not open attachments from an unknown source without checking with my teacher.

I agree that any of my school work may appear on the school web site.

I understand that all of my work and internet activity on school ICT equipment can be monitored and that there are consequences if I do not use the equipment sensibly, safely and responsibly.

Parent/Carer's Signature:

Date:

Child's Signature:

Pupil Name:

Appendix 4

Staff ICT Acceptable Use Policy

To ensure that you are fully aware of your professional responsibilities when using ICT in school, you are asked to read and sign this code of conduct. You should consult the school's e-safety policy for further information and clarification.

Access

- The ICT systems are school property and I understand that it is a criminal offence to use a device for a purpose not permitted by its owner.
- I understand that ICT may not be used for private purposes, without specific permission from the head teacher.
- I will respect system security and I will not disclose any password or security information to anyone other than an appropriate system manager.
- I will not attempt to bypass any devices or network settings.
- I will not install any software or hardware without permission.
- I will respect copyright and intellectual property rights.
- I will only use my school email address for school business.

Communication

- I will ensure that electronic communications with pupils including email, instant messaging and social networking are compatible with my professional role and that messages cannot be misunderstood or misinterpreted.
- I will ensure my social network privacy settings prevent others viewing my personal details and materials and ensure that I never accept or request invites or friend requests from any pupils on line.

Storage

- I will ensure that personal data is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely using school owned secure systems.
- I will only use photographs/videos taken of pupils or staff with their permission.

Use of Personal Equipment

- I understand I must not use personal, portable or 'cloud' media for storage of images and videos without the express permission of the Headteacher.
- I will not use my mobile phone or personal device for anything other than school purposes during lesson time and when on duty.

Staying Safe Online

- I will report any incidents of concern regarding children's safety to the safeguarding officer.
- I will promote e-safety with students in my care and will help them to develop a responsible attitude to system use and to the content they access or create.
- I will adhere to the Teachers Code of Conduct when using social networking and will not bring my professional role into disrepute.
- I will support the school approach to online safety and not deliberately upload or add any images, videos, sounds or text that could upset or offend any member of the school community.
- I will advise pupils to keep evidence of any inappropriate use by taking screen shots, saving emails and texts. **I will not ask students to forward images or inappropriate content to my personal mobile phone, to my school account or electronic device.**

The school or SRS may exercise its right to monitor the use of the school's information systems, including Internet access, the interception of e-mail and the deletion of inappropriate materials where it believes unauthorised use of the school's information system may be taking place, or the system may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound.

I have read, understood and agree with the Acceptable Use Policy.

Signed: Date:

Print Name:.....

Appendix 5

Useful websites

www.thinkuknow.co.uk

www.wisekids.org.uk

www.anti-bullyingalliance.org.uk

www.ceop.gov.uk

www.kidsmart.org.uk

www.meiccymru.org

www.hwb.wales.gov.uk

www.schoolbeat.org

www.learning.wales.gov.uk

<http://wales.gov.uk/topics/educationandskills/publications/circulars/antibullying/?lang=en>

Acts Relating to the Protection of Personal Data

Data Protection Act 1998

http://www.opsi.gov.uk/acts/acts1998/ukpga_19980029_en_1

The Freedom of Information Act 200

http://www.ico.gov.uk/for_organisations/freedom_of_information_guide.aspx

Creative Commons- non-profit copyright organization

www.creativecommons.org

Appendix 6

Glossary

Social networking

A dedicated website or other application which enables users to communicate with each other by posting information, comments, messages, images, etc...

Usually free to join and open to young people and adults (sites such as Facebook and Bebo have a minimum age limit of 13 for registered users; MySpace's age restriction is 14)

Examples of social networking sites are as follows, but this is not a complete list!

- Facebook,
- MySpace,
- Twitter,
- Bebo,
- ClubPenguin,
- Poptropicana,
- Habbo,
- Neopets,
- Stardoll,
- Moshimonsters
- Utube
- Blogs

Dropbox

Dropbox is a [personal cloud storage](#) service (sometimes referred to as an online backup service) that is frequently used for [file sharing](#) and collaboration.

Cloud

iCloud allows subscribers to save their address book, calendar, notes, Safari bookmarks and photos on Apple's servers -- changes and additions to one Apple device can be pushed to the subscriber's other registered Apple devices.

Hwb+

The first phase of the new all Wales Learning Platform. Together with the Education Wales site on iTunesU, Hwb will become a growing collection of resources, a place to share best practice and contribute to professional learning community sites.

Hwb+ will provide a secure learning platform for schools with avatars, fun themes, Web 2.0 tools such as blogs and wikis and much more. Hwb+ will also include Microsoft Office 365. Schools will be able to use Hwb+ for all their communications, to collaborate and to work on curriculum through projects and assignments. Hwb+ will be available free to all Welsh schools.

Cyber bullying

Cyberbullying can be defined as the use of information and communication technology (ICT), particularly mobile phones and the internet (including social networking sites, blogs, e-mail, video and instant messaging), to deliberately upset someone else.

The Anti-Bullying Alliance defines it as:

'... an aggressive, intentional act carried out by a group or individual, using electronic forms of contact, repeatedly and over time against a victim who cannot easily defend him or herself.'

(www.anti-bullyingalliance.org.uk)

Bullying

Bullying is a "persistent attempt to hurt or humiliate someone and often involves an imbalance of power where a person or group of people repeatedly and intentionally cause emotional and / or physical harm to another person or group of people.

Isolated incidents of hurtful behaviour, teasing, arguments or falling out between individuals of equal power should not be seen as bullying."

Foundation Phase

*These rules help us to stay
safe on the Internet*

Think then Click

Key Stage 2

Think then Click

