Wales Primary School
MAKING A DIFFERENCE

E-Safety Policy

Our aim is that our children and our parents are able to participate online and have the wisdom to make wise choices, empowering them to be resilient and have the responsibility for their own behaviour.

We love the internet and it's important that we all know how to behave online. We love technology and our lives seem permanently connected in one way or another nowadays. We should embrace this but it can be hard with so many negative stories in the news about risks, dangers and online bullying.

It is so important that we are able to manage our online activity in a safe way. This will enable us to enjoy the internet but keep ourselves safe from any of the dangers. Our curriculum content; enrichment activities; special assemblies; extra curricular clubs; parent, governor and staff training events and E Safety Cadets ensure that a persistent message of safe internet use is consistently heard by all the members our school community.

E-Safety

E-Safety encompasses the use of new technologies, internet and electronic communications such as mobile phones, collaboration tools and personal publishing. It highlights the need to educate pupils about benefits and risks of using technology and provides safeguards and awareness for users to enable them to control their online experience. This will include current new technology and how we should behave when using them. The policy reflects the need to raise awareness of the safety issues associated with electronic communications as a whole including cyberbullying and working online. The school's policy will operate in conjunction with other policies including those for Behaviour, Bullying, Curriculum, Data Protection and Security.

End to End E-Safety

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.
- Sound implementation of e-safety policy in both administration and curriculum, including secure school network design and use.
- Safe and secure broadband from Rotherham LA network including the effective management of filtering.
- National Education Network standards and specifications.

School e-Safety Policy

Writing and reviewing the e-safety policy. The e-Safety policy relates to other policies including those for ICT, Bullying and for Child Protection

- The ICT Co-ordinator and the Headteacher regularly review the e-safety policy.
- Our E-Safety Policy has been written by the school, building on government guidance. It has been agreed by all staff and approved by governors.
- The E-Safety Policy and it implementation will be review annually.

Teaching and Learning

Why Internet use is important

- 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.

Internet use will enhance learning

- The school internet access will be designed expressly for pupil use and will include filtering appropriate to the age of the pupils.
- Pupils will be taught what internet use is acceptable and what is not and given clear objectives for Internet use.
- Pupils will be educated in the effective use of the internet in research, including the skills of knowledge location, retrieval and evaluation,

Pupils will be taught how to evaluate Internet content

- The school will ensure that the use of Internet derived by staff and pupils complies with copyright law.
- Pupils should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

Curriculum Content

- EYFS and Key Stage 1 use Purple Mash and Hector's World to promote key E-Safety messages in the classroom
- Key Stage 2 use Purple Mash and Think You Know online content to promote key E-Safety messages
- E-Safety is promoted and key messages are shared in regular whole school safety assemblies
- Our children have access to Rotherham's Power specialist E-Safety advice and enrichment sessions
- Rotherham Power train Year 6 E-Safety Cadets who deliver safety assemblies and run ICT clubs for our children to develop their knowledge and understanding of effective E-Safety
- Extra-curricular ICT clubs promote E-Safety
- Children are informed about CEOPS and a link is available on our school website for children to report unsafe behaviour and actions
- Children are informed and taught about Bullying and Cyber bullying via PSHCE lessons, visits (such as Crucial Crew), visitors (E-Safety Power Team), visits (CLC) and assemblies

<u>Managing Internet Access</u>

Information systems security

- School ICT systems capacity and security will be reviewed regularly.
- Virus protection will be updated regularly.
- Passwords are kept private and not shared

E-mail

- Pupils may only use approved e-mail accounts on the school system.
- Pupils must immediately tell a teacher if they receive offensive e-mail
- Pupils must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission.
- E-mail sent to an external organisation should be written carefully and authorised before sending, in the same way as a letter written on school headed paper.
- The forwarding of chain letters is not permitted.

Published content and the school web site

- The contact details on the Web site should be the school address number. Staff or pupils personal information will not be published.
- The Headteacher will take overall editorial responsibility.

Publishing pupils' images and work

- Photographs that include pupils will be selected carefully.
- Pupils full names will not be used anywhere on the Web site.
- Written permission from parents or carers will be obtained before information and photographs are published on the school web site.

Social networking and personal publishing

- The school will block/filter access to social networking sites.
- Newsgroups will be blocked unless a specific use is approved
- Pupils will be advised never to give out personal details of any pupils or their location.
- Pupils and parents will be advised that the use of social networking is appropriate for primary aged pupils.

Managing filtering

- The school will work with LA, DfE and the Internet Server systems to protect pupils are reviewed and improved.
- If staff or pupils discover an unsuitable site, it must be reported.

Staff will ensure that regular checks are made. Managing videoconferencing

- IP videoconferencing should use the educational broadband network to ensure quality of service and security rather than the Internet.
- Pupils should ask permission from the supervising teacher before making or answering a videoconference call.
- Videoconferencing will be appropriately supervised for the pupil's age.

Managing emerging technologies

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in the school is allowed.
- Mobile phones are allowed on school premises however due to the development of 'smart technology' parents will be asked to refrain from using them around children. If a parent persists then they may be asked to leave the school premises. Staff must use their phone in the designated areas of school where children are not present.
- Children have to hand mobile phones into the office before school starts and collect them at the end of the school day. Any child found in possession of a mobile phone in the school grounds will have it confiscated by a member of the SLT and their parents informed immediately.
- The sending of abusive or inappropriate text messages is forbidden.
- No member of staff should use their personal email address for contact with pupils, parents or governors on school related matters – their personal school email or the school email account should only be used.
- Staff have been advised on appropriate personal security measures when using the internet or personal mobile phones.

Protecting personal data

- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 as outlined in the Data Protection Policy.

Policy Decisions

Authorising Internet access

- All staff must read and sign the 'Acceptable ICT Use Agreement' before using any school ICT resource.
- The school will keep a record of all staff and pupils who are granted Internet access. The record will be kept up to date, for instance a member of staff may leave or a pupil's access be withdrawn.
- At EYFS access to the internet will be by adult demonstration and some directly supervised access to specific approved on-line materials.
- At Key stage 1, access to the Internet will be by adult demonstration with directly supervised access to specific, approved on-line materials.
- At Key Stage 2, access will be by adult demonstration, supervised access to specific approved on-line materials leading to developing greater independence through the supervised researching of and accessing of varied materials on the internet.
- Parents will be asked to sign and return a consent form before a child can use and access ICT resources and the internet.

Assessing Risks

- The school with take all reasonable precautions to ensure that users access only appropriate material, however, due to the international scale and linked nature of Internet content, it is not possible to guarantee that the material will never appear on a school computer. The school cannot accept liability for the material accessed, or any consequences of Internet access.
- The school will audit ICT provision to establish if the E-Safety policy is adequate and that its implementation is effective.

Handling E-Safety complaints

- Complaints of Internet misuse will be dealt with by a senior member of staff (as outlined in the appended flow chart)
- Any complaint about staff misuse must be referred to the Headteacher
- Complaints of a child protection nature must be dealt with school child protection procedures.
- Pupils and parents will be informed of the complaint procedure.

Communication Policy

Introducing the E-Safety policy to pupils

- E-safety rules will be posted in all classrooms and discussed with the pupils at the start of each year.
- Pupils will be informed that network and Internet use will be monitored.

Staff and the E-Safety Policy

- All staff will be given the E-Safety policy and its importance explained.
- Staff should be aware that the Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.

Enlisting parents support

- Parent's attention will be drawn to the E-Safety Policy in newsletters, children's work, the school prospectus and on the school website.

Date written: November 2017
Review Date: November 2018

Staff Acceptable ICT Use Agreement

ICT (including data) and the related technologies such as e-mail, the internet, iPad and mobile devices are an expected part of our daily working life in school. This policy is designed to ensure that all staff are aware of their professional responsibilities when using any form of ICT. All staff are expected to sign this policy and adhere at all times to its contents. Any concerns or clarification should be discussed with the Headteacher.

- I will only use the school's email / Internet / Server and any related technologies for professional purposes or for uses deemed acceptable by the Head or Governing Board
- I will comply with the ICT system security and not disclose any passwords provided to me by the school or other related authorities
- I will ensure that all electronic communications with pupils and staff are compatible with my professional role
- I will not give out my own personal details, such as mobile phone number, personal e-mail address, personal Twitter account, or any other social media link, to pupils
- I will only use the approved, secure e-mail system(s) for any school business
- I will ensure that personal data is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely. Personal data can only be taken out of school or accessed remotely when authorised by the Head or Governing Board.
- I will not install any hardware or software without permission of the ICT Coordinator or the Headteacher.
- I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory
- Images of pupils and/ or staff will only be taken, stored and used for professional purposes in line with school policy and with written consent of the parent, carer or staff member
- Images will not be distributed outside the school network without the permission of the parent/ carer, member of staff or Headteacher
- I will support the school approach to online safety and not deliberately upload or add any images, video, sounds or text that could upset any member of the school community
- I understand that all my use of the Internet and other related technologies can be monitored and logged and can be made available, on request, to the Headteacher
- I will respect copyright and intellectual property rights
- I will ensure that my online activity, both in school and outside school, will not bring the school, my professional role or that of others into disrepute
- I will support and promote the school's e-Safety and Data Protection policies and help pupils to be safe and responsible in their use of ICT and related technologies

User Signature

I agree to follow this code of conduct and to support the safe and secure use of ICT.

Signature …… Date……

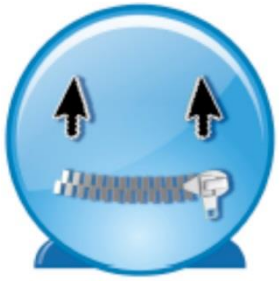
Full Name ……(printed)

Job title……

Wales Primary School
MAKING A DIFFERENCE

Wales Primary School
Acceptable Use of ICT Agreement/E-Safety Rules For Children

- **I will only use ICT in school for school purposes**
- **I will only use my class e-mail address or my own school e-mail address when e-mailing**
- **I will only open e-mail attachments from people I know, or who my teacher has approved**
- **I will not tell other people my ICT passwords**
- **I will only open/delete my own files**
- **I will not bring software, CDs or ICT equipment into school without permission**
- **I will only use the Internet after being given permission from a teacher**
- **I will make sure that all ICT contact with other children and adults is responsible, polite and sensible**
- **I will not deliberately look for, save or send anything that could be upsetting or not allowed at school. If I accidentally find anything like this, I will close the screen and tell a teacher immediately**
- **I will not give out my own details such as my name, phone number or home address**
- **I will not use technology in school time to arrange to meet someone unless this is part of a school project approved by a teacher and a responsible adult comes with me**
- **I will be responsible for my behaviour when using ICT because I know that these rules are to keep me safe**
- **I know that the school may check my use of ICT and monitor the Internet sites I have visited, and that my parent/carer will be contacted if a member of school staff is concerned about my E-Safety**



ZIP IT

Keep your personal stuff private and think about what you say and do online.

BLOCK IT

Block people who send nasty messages and don't open unknown links and attachments.

FLAG IT

Flag up with someone you trust if anything upsets you or if someone asks to meet you offline.

Be smart on the internet

Childnet International

www.childnet.com

S SAFE Keep safe by being careful not to give out personal information – such as your full name, email address, phone number, home address, photos or school name – to people you are chatting with online.

M MEETING Meeting someone you have only been in touch with online can be dangerous. Only do so with your parents' or carers' permission and even then only when they can be present.

A ACCEPTING Accepting emails, IM messages, or opening files, pictures or texts from people you don't know or trust can lead to problems – they may contain viruses or nasty messages!

R RELIABLE Information you find on the internet may not be true, or someone online may be lying about who they are.

T TELL Tell your parent, carer or a trusted adult if someone or something makes you feel uncomfortable or worried, or if you or someone you know is being bullied online.

You can report online abuse to the police at www.thinkuknow.co.uk

THINK U KNOW

www.kidsmart.org.uk

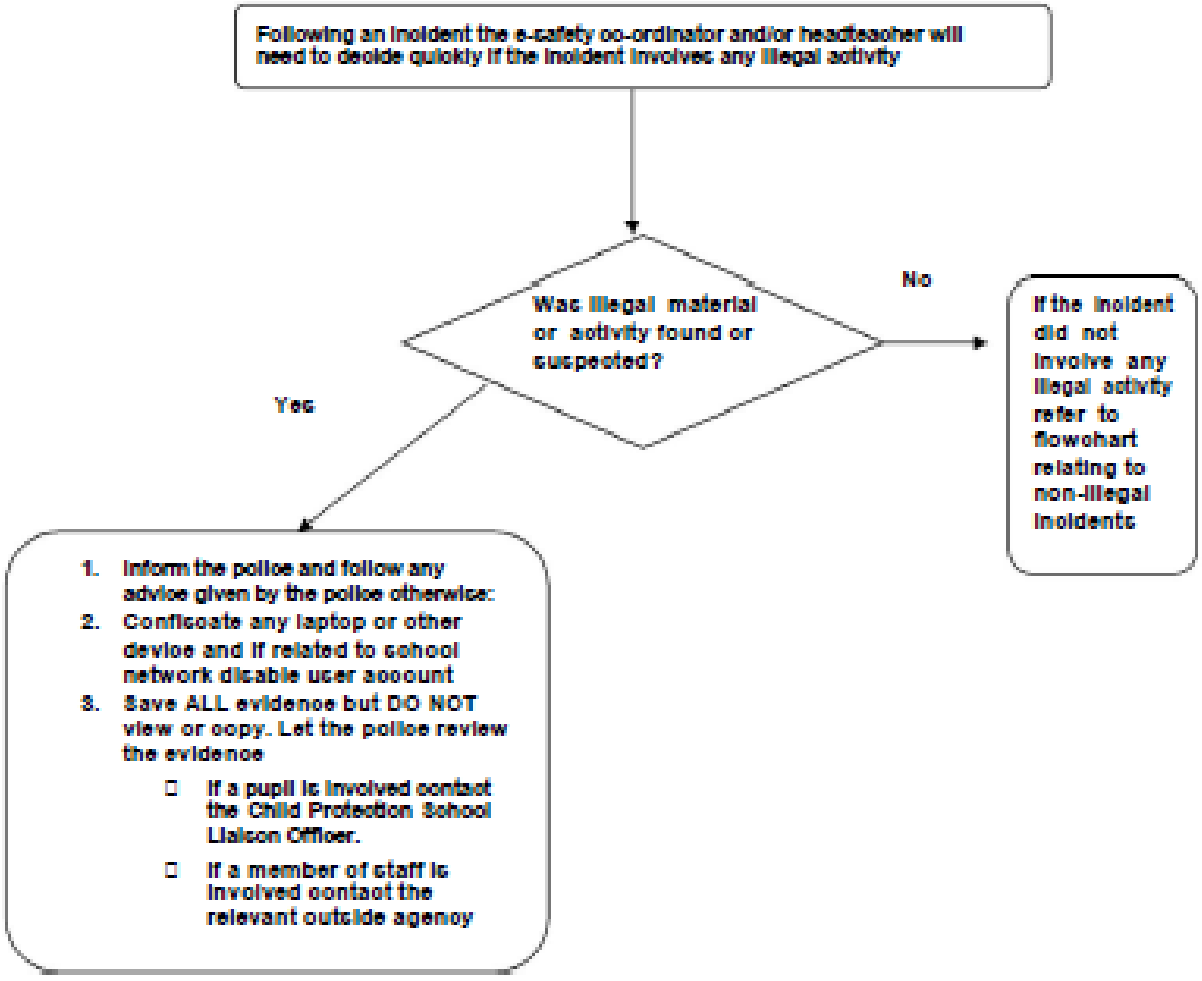
KidSMART

Visit Childnet's Kidsmart website to play interactive games and test your online safety knowledge. You can also share your favourite websites and online safety tips by Joining Hands with people all around the world.

Flowchart for Managing an e-safety incident involving illegal activity

Illegal means something against the law, such as:

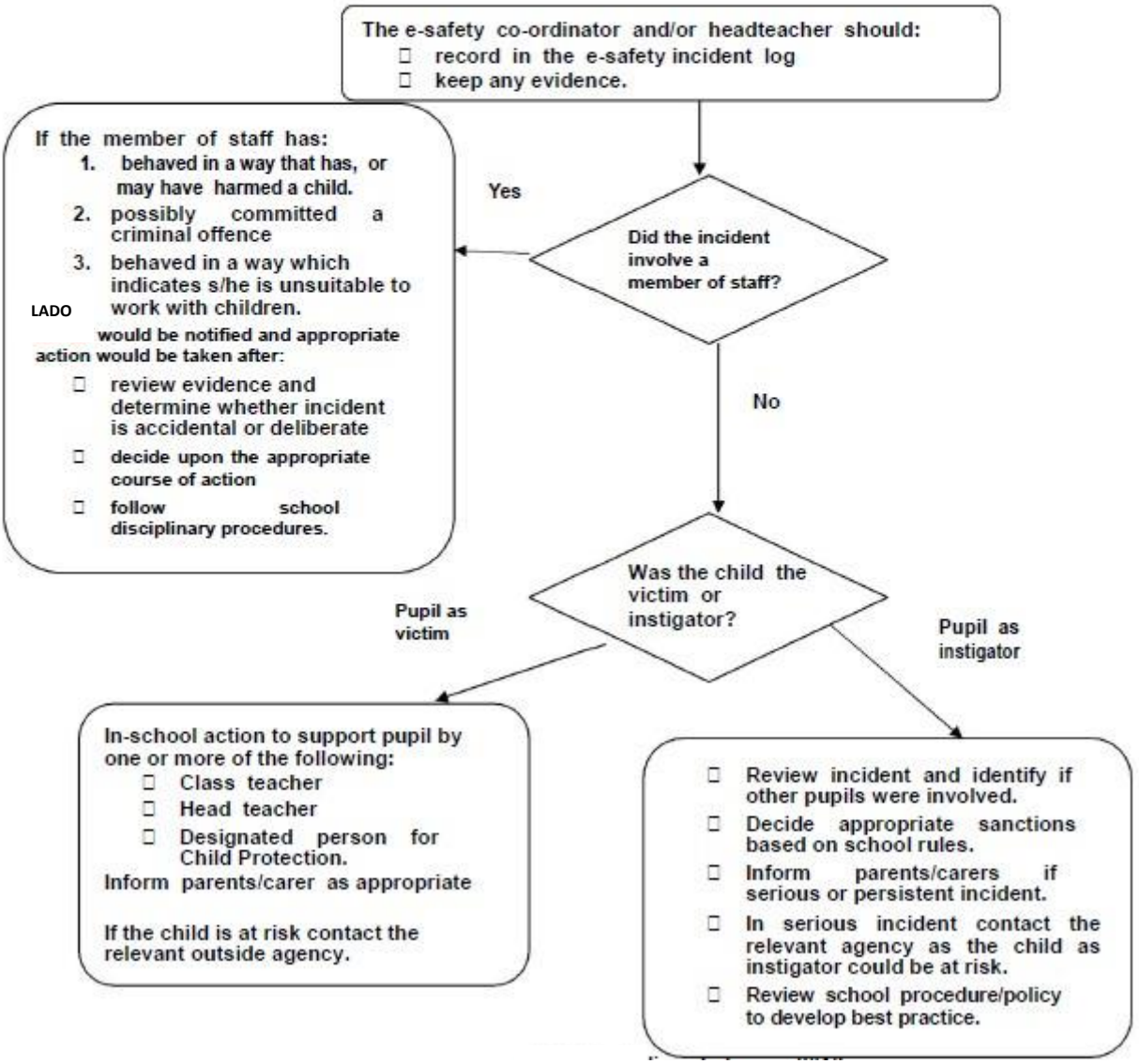
- downloading child pornography
- passing onto others images or video containing child pornography
- inciting racial or religious hatred
- promoting illegal acts



Flowchart for Managing an e-safety incident not involving any illegal activity

Incidents not involving any illegal activity, such as:

- using another person's user name and password
- accessing websites which are against school policy
- using a mobile phone to take video during a lesson
- using the technology to upset or bully (in extreme cases this could be illegal)



WALES PRIMARY SCHOOL E SAFETY INCIDENT LOG						
Date / Time / Location	Type • **Content** • **Conduct** • **Contact** • **Commerce**	Name of child / staff involved	System Details	Incident	Action	Outcome
	Content Conduct Contact Commerce					
	Content Conduct Contact Commerce					
	Content Conduct Contact Commerce					
	Content Conduct Contact Commerce					
	Content Conduct Contact Commerce					
	Content Conduct Contact Commerce					