Gwasanaeth TGCh Ysgolion a'r Gymuned
01970 633678

Ceredigion

Ceredigion e-Safety Guidance

Ceredigion County Council has approved this core e-Safety Guidance, which can be used by schools as a template to construct their own policies.

CONTENTS

1. Guidance

The Internet is an essential element in 21st century life for education, business and social interaction. Schools have a duty to provide students with high-quality Internet access as part of their learning experience. Internet use is a part of the statutory curriculum and a necessary learning tool for staff and students.

Ceredigion County Councils' e-safety Guidance is a collaboration of relevant e-safety policy templates. It provides a detailed discussion of e-safety issues and links to further information. It is revised annually and should be read in conjunction with the excellent material from the Child Exploitation and Online Protection (CEOP) centre.

However each school **must** maintain its own e-Safety Policy in order to make its own decisions on balancing educational benefit with potential risk. The ICT advisory service is available to support you in this process.

A school's e-Safety Policy must cover the safe use of internet and electronic communications technologies such as mobile phones and wireless connectivity. The policy will highlight the need to educate children and young people about the benefits and risks of using new technologies both in and away from school. It will also provide safeguards and rules to guide all users whether staff or student in their online experiences.

The school's e-safety policy will operate in conjunction with other policies including those for Student Behaviour, Bullying, Curriculum, Data Protection Safeguarding Children and Security plus any Home-School Agreement.

To assist schools in writing and maintaining their own policies we have grouped the policy templates into three main categories; Data and Security, Acceptable Use Policies, Infrastructure and Technology. Electronic copies of these templates are available on our ICT Support Site, (http://addysg.cerenet.org.uk/).

A map of all Policy Templates can be found on the next page.

1.1 Effective Practice in e-Safety

E-Safety depends on effective practice in each of the following areas:

- Education for responsible ICT use by staff and students;
- A comprehensive, agreed and implemented e-Safety Policy;
- Secure, filtered broadband from Ceredigion County Council network.
- Regular reviews on Internet Filtering reports.
- Schools should encourage parents to discuss e-safety issues with their children and to take an interest in their internet activities
- Parents' and carers' attention will be drawn to the School e-Safety Policy in newsletters, the school brochure and on the school Web site.
- The school will maintain a list of e-safety resources for parents/carers.
- The school will ask all new parents to sign the parent /pupil acceptable use policy agreement when they register their child with the school.

1.2 Who are your contacts / Seeking Advice

- Kay Morris – ICT Advisory Teacher 01970 633746
- Sera Llywelyn - Child Protection Officer 01970 633624
- Schools and Community ICT Service 01970 633678
- Alan Morris - Computer Development Manager 01970 633667
- http://addysg.cerenet.org.uk/

2. E-Safety Audit

This self-audit should be completed by the member of the Senior Leadership Team (SLT) responsible for e-safety policy. Staff that would contribute to the audit including: Designated Child Protection Coordinator, SENCO, e-Safety Coordinator and Head Teacher.

	The e-Safety Coordinator is:	
	Has the school an e-Safety Policy?	**Y/N**
	The e-Safety Policy was revised by:	
	Date of latest update (at least annual):	
	The school Governor Representative e-Safety co-ordinator is:	
	The responsible member of the Senior Leadership Team is:	
	The school e-safety policy was agreed by governors on:	
	The next review date is (at least annually):	
	The policy is available for staff at:	
	The policy is available for parents/carers at:	
	The Designated Child Protection Coordinator is:	
	Has e-safety training been provided for staff?	**Y/N**
	Are staff aware of e-safety materials from CEOP?	**Y/N**
	Are e-safety rules displayed in all rooms where computers are used and expressed in a form that is accessible to all students?	**Y/N**
	Are all students aware of the School's e-Safety Rules?	**Y/N**
	Has e-safety training been provided for students?	**Y/N**
	Is personal data collected, stored and used according to the principles of the Data Protection Act?	**Y/N**
2.3	Is there a clear procedure for a response to an incident of concern?	**Y/N**
2.7	Do all staff sign an Acceptable Use Policy for ICT on appointment?	**Y/N**
2.7	Do students sign and return an agreement that complies with the School Acceptable Use Policy?	**Y/N**
2.7	Do parents/carers sign and return an agreement that their child will comply with the School Acceptable Use Policy?	**Y/N**
2.8	Are staff, students, parents/carers and visitors aware that network and Internet use is closely monitored and individual usage can be traced?	**Y/N**
2.8	Are staff and students aware of the correct and safe usage of email and social media?	**Y/N**
2.6	Are staff aware of Data Security requirements?	**Y/N**

2.1 Introducing the e-safety policy to students

Best practice for the introduction of e-safety to students might include;

- E-Safety rules will be posted in all rooms where ICT devices are used.
- Students will be informed that network and Internet use will be monitored and appropriately followed up.
- Acceptable use will be explained and procedures for dealing with issues documented
- A programme of training in e-Safety will be developed.
- E-Safety training will be embedded within the ICT scheme of work and/or the Personal Social Education (PSE) curriculum.

2.2 Staff and the e-Safety policy

Best practice might include the following;

- All staff will be given the School e-Safety Policy and its importance explained.
- Staff must be informed that network and Internet traffic can be monitored and traced to the individual user.
- Staff should have clear procedures for reporting issues.
- Staff should understand that phone or online communications with students can occasionally lead to misunderstandings or even malicious accusations. Staff must take care always to maintain a professional relationship.
- Staff will always use a child friendly safe search engine and safe search options when accessing the web with students.
- Staff should sign the schools Staff Acceptable Use Policy.
- Staff should have access to e-safety training and be made aware of online resources.

2.3 Handling an E-Safety incident

Best practice might include the following;

- Clear guidance on how to record and handle an e-safety issue.
- Complaints of ICT misuse will be dealt with by a senior member of staff.
- Any complaint about staff misuse must be referred to the Head Teacher.
- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.
- Students and parents will be informed of the complaints procedure.
- Students and parents will be informed of consequences for students misusing the Internet.
- Discussions will be held with the Community Police Officer to establish procedures for handling potentially illegal issues.

2.4 Reporting an E-Safety incident

The Child Protection or e-Safety Coordinator can provide guidance should you be concerned about ICT or Internet misuse by a child, young person or member of staff.

The flowchart included in the appendix illustrates the approach to resolving an incident of concern. This diagram should not be used in isolation and the Education and Children's Services and the Local Safeguarding Children Board can provide supporting documents to assist schools when responding to incidents.

2.5 Assessing risks

Best practice might include the following;

- The school will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a computer connected to the school network. Neither the school nor Ceredigion County Council can accept liability for any material accessed, or any consequences of Internet access.
- The school should audit ICT use to establish if the e-safety policy is adequate and that the implementation of the e-safety policy is appropriate and effective.

2.6 Data and Account Security

Schools should actively maintain the following policies;

- **School Data Handling Policy**
  This policy avoids or at least minimises the risk of personal data breaches. A breach may arise from a theft, a deliberate attack on your systems, the unauthorised use of personal data by a member of staff, accidental loss, or equipment failure.

- **School Password Security Policy / Policy Template**
  This policy will provide guidance on how the school can uphold a safe and secure username and password system.

- **Social Media Policy Template**
  This policy will provide guidance on how to use social media safely in an educational environment.

Templates for the above policies are available on; http://addysq.cerenet.org.uk/

2.7 Acceptable Use Policies

Schools should actively maintain the following policies;

- **Staff Acceptable Use Policy Agreement**
- **Student Acceptable Use Policy Agreement**
- **Parent Acceptable Use Policy Agreement**

Acceptable Use Policies are intended to ensure that;

a. staff and young people will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.

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

c. Parents and carers are aware of the importance of e-safety and are involved in the education and guidance of young people with regard to their on-line behaviour.

Templates for the above policies are available on; http://addysq.cerenet.org.uk/

2.8 Infrastucture and Technology

Schools should actively maintain the following policies;

- **Internet Filtering in schools Policy**
  This policy will provide guidance on how best to ensure Internet Filtering is managed within a school environment.

  Best practice might include the following;

  - If staff or students discover an unsuitable site, it must be reported to the Schools and Community ICT Service through the appropriate channels.
  - Senior staff will ensure that regular checks are made to ensure that the filtering is appropriate, effective and reasonable.

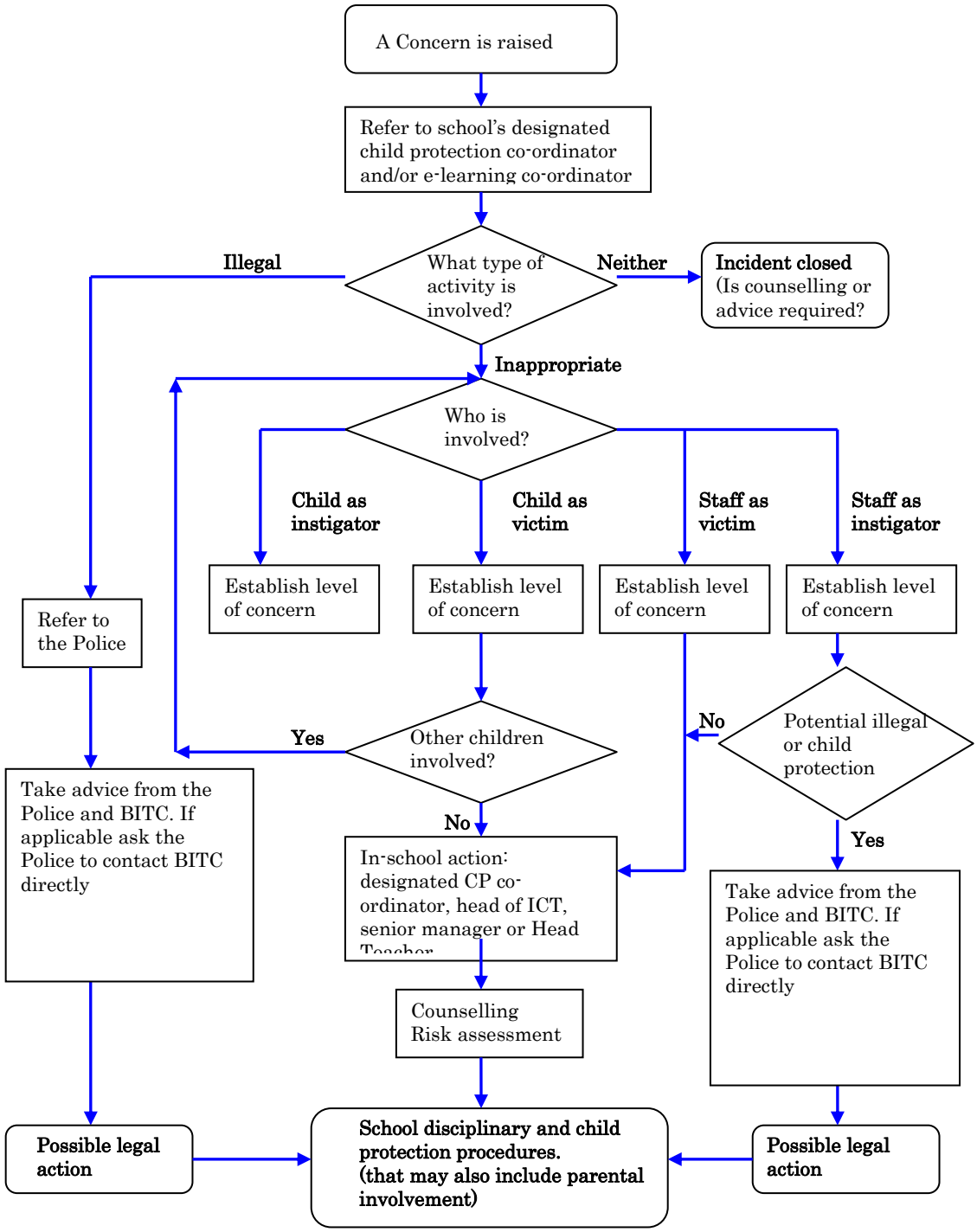
- **E-communication Policy / Policy Template**
  This policy will provide guidance on how to develop effective practice and to use e-communications responsibly as well as understanding network etiquette (netiquette).

- **BYOD Policy**
  If supported, this policy will provide guidance on how 'Bring Your Own Device' could be used safely and securely within the school network.

  Templates for the above policies are available on; http://addysg.cerenet.org.uk/

Appendix 1: Internet use - Possible teaching and learning activities	
Activities	**Key e-safety issues**
Creating web directories to provide easy access to suitable websites.	Parental consent should be sought. Students should be supervised. Students should be directed to specific, approved on-line materials.
Using search engines to access information from a range of websites.	Filtering must be active and checked frequently. Parental consent should be sought. Students should be supervised. Students should be taught what internet use is acceptable and what to do if they access material they are uncomfortable with.
Exchanging information with other students and asking questions of experts via e-mail or blogs.	Students should only use approved e-mail accounts or blogs. Students should never give out personal information.
Publishing students' work on school and other websites.	Pupil and parental consent should be sought prior to publication. Students' full names and other personal information should be omitted. Students' work should only be published on 'moderated sites'.
Publishing images including photographs of students.	Parental consent for publication of photographs should be sought. Photographs should not enable individual students to be identified. File names should not refer to the pupil by name. Staff must ensure that published images do not breach copyright laws.
Communicating ideas within chat rooms or online forums.	Only chat rooms dedicated to educational use and that are moderated should be used. Access to other social networking sites should be restricted inline with the social media policy. Students should never give out personal information.
Audio and video conferencing to gather information and share students' work.	Students should be supervised. Internal teacher led systems such as Big Blue Button reduce risks.

Appendix 2: Resolving an incident of concern



Appendix 3: Useful resources for teachers

Ceredigion ICT Support Centre	http://addysg.cerenet.org.uk/
BBC Stay Safe	www.bbc.co.uk/cbbc/help/safesurfing/
Chat Danger	www.chatdanger.com/
Child Exploitation and Online Protection Centre	www.ceop.gov.uk/
Childnet	www.childnet-int.org/
Cyber Café	http://thinkuknow.co.uk/8_10/cybercafe/cafe/base.aspx
Digizen	www.digizen.org/
Kent e-Safety Policy and Guidance, Posters etc	www.clusterweb.org.uk/kcn/e-safety_home.cfm
Kidsmart	www.kidsmart.org.uk/
Think U Know	www.thinkuknow.co.uk/

Appendix 4: Useful resources for parents

Childnet International "Know It All" CD	http://publications.teachernet.gov.uk
Family Online Safe Institute	www.fosi.org
Internet Watch Foundation	www.iwf.org.uk
Kent leaflet for parents: Children, ICT & e-Safety	www.kented.org.uk/ngfl/ict/safety.htm
Internet Safety Zone	www.internetsafetyzone.com

Map of Policy Templates