Alltwen Primary School
E-Safety Policy

C O N T E N T S

Introduction

Alltwen Primary School E-Safety Policy is based on the Neath Port Talbot County Borough Council (NPTCBC) e-Safety Policy Guidance, which provides a detailed discussion of e-safety issues and links to further information.

The Policy covers 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 staff, pupils and visitors in their online experiences.

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

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 pupils;
- A comprehensive, agreed and implemented E-Safety Policy;
- Secure, filtered broadband from the Neath Port Talbot Network;
- A school network that complies with the Lifelong Learning Network Wales standards and specifications.

E-Safety Audit – Primary / Special

Has the school an E-Safety Policy that complies with NPT guidance?	**Y**
The school E-Safety policy was agreed by governors on: 14.01.26	
The policy is available for staff at: School Office	
The policy is available for parents/carers at: School Office and School Website	
The responsible member of the Senior Leadership Team is: Mrs G. Herbert	
The responsible member of the Governing Body is: Mrs D. Moran	
The Designated Child Protection Coordinator is: Mrs G. Herbert	
The E-Safety Coordinator is: Mr G Hazel	
Has E-Safety training been provided for both pupils and staff?	**Y**
Is there a clear procedure for a response to an incident of concern?	**Y**
Have e-safety materials from CommonSense Education been obtained?	**Y**
Do all staff have updated training and sign an Acceptable Use Policy for ICT each year?	**Y**
Are all pupils aware of the School's E-Safety Rules?	**Y**
Are E-Safety rules displayed in all rooms where computers are used and expressed in a form that is accessible to all pupils?	**Y**
Are parents notified of acceptable use behaviour when using school devices?	**Y**
Are staff, pupils, parents/carers and visitors aware that network and Internet use is closely monitored and individual usage can be traced?	**Y**
Is personal data collected, stored and used according to the principles of the Data Protection Act?	**Y**
Have parents signed consent forms for their child to access Hwb and Classdojo?	**Y**

1. School E-Safety policy

The E-Safety Policy relates to other policies including those for ICT, bullying and for child protection.

- The school has appointed an e-Safety Coordinator Mr G Hazel
  The School Designated Child Protection Coordinator is Mrs. G Herbert.

- Our E-Safety Policy has been written by the school, building on the NPTCBC E-Safety Policy and government guidance. It has been agreed by senior management and approved by governors.

2. Teaching and learning

Why the Internet and digital communications are important

- The Internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide pupils 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 benefit education

- Inclusion in the Lifelong Learning Network Wales which connects schools in NPT

- Access to world-wide educational resources including museums and art galleries

- Collaboration across support services and professional associations

- Exchange of curriculum and administration data with the Local Authority and the Welsh Assembly Government

- A range of suitable websites and programmes (eg Hwb) maybe used during Blended Learning in school and at home

Internet use will enhance learning as focused teaching as well as incorporated during DCF lessons

- The school Internet access will be designed expressly for pupil use and will include filtering appropriate to the age of pupils.

- Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.

- Pupils will undertake E-Safety lessons every half term as well as being incorporated into a range of DCF lessons (Citizenship) throughout the year.

- 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 shown how to publish and present information to a wider audience.

Pupils will be taught how to evaluate Internet content

- The school will ensure that the use of Internet materials derived by staff and pupils complies with copyright law.

- Pupils will be taught the importance of cross-checking information before accepting its accuracy.

- Pupils will be taught how to report unpleasant Internet content to the teacher. Teachers to follow correct procedures, which are in place, to report this material.

3. Managing Information Systems

Information system security

- School ICT systems security will be reviewed regularly.

- Virus protection will be updated regularly.

- Security strategies will be discussed with the Local Authority.

E-mail

- Pupils may only use an approved e-mail account on the school system e.g.-Hwb.

- Pupils must immediately tell a teacher if they receive offensive e-mail, emails from an unknown person or any emails which contain attachments.

- In e-mail communication, pupils must not reveal their personal details or those of others, or arrange to meet anyone without specific permission- think SMART (Safe, Meeting, Accepting, Reliable, Tell)

- The forwarding of chain letters is not permitted.

- Incoming e-mail should be treated as suspicious and attachments not opened unless the author is known.

- The school should consider how e-mail from pupils to external bodies is presented and controlled.

Published content and the school web site

- Staff or pupil personal contact information will not be published. The contact details given online are contact details of the school office eg: phone number

and school email address.

- There will be a designated person within the school who will take overall editorial responsibility and ensure that content is up to date, accurate and appropriate.

Publishing pupil's images on the school website and using class dojo.

- Parents consent needs to be obtained before images of their child can be shared on Classdojo and on the school website. This information is obtained during our first 'Meet the teacher' session each September. Parents will specify which information they consent to be shared eg- just image, just name, both image and name or neither.

- Parents should be clearly informed of the school policy on image taking and publishing, both on school and independent electronic repositories.

Social networking and personal publishing

- Classdojo accounts have been created and are closed accounts. Parental consent has been gathered first before sharing of pictures. Personalised QR codes have been sent home to parents so they can access their child's account.

Managing filtering

- If staff or pupils come across unsuitable on-line materials, the site must be reported to the E-Safety Coordinator and follow the 'Reporting Incidents of E-Safety Procedures'.

- E-safety Coordinator will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

Managing videoconferencing & webcam use

- During Blended Learning, clear guidelines are given to both pupils and parents of the correct way to conduct themselves on camera and during online sessions. If both pupils or parents do not follow the given guidelines, they will be asked to leave the session.

EG- camera on at all times, dress appropriately, no recording of sessions, appropriate use of chat bar.

Managing emerging technologies

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

- Mobile phones, for personal use, are allowed on school premises but only used during break/playtimes. Not during lesson time.

- **No** games machines including the Sony Play station, Microsoft Xbox and others that have Internet access which may not include filtering, are allowed on school premises.

- The appropriate use of Learning Platforms will be discussed as the technology becomes available within the school.

Protecting personal data

- Protocol of protecting personal information will be followed using the GDPR guidelines and policy.

4. Policy Decisions

Authorising Internet Access

- All staff will undertake a refresher session on Acceptable use of school devices and any updates to the Social Media policy, every September. All staff must read and sign the Acceptable Use Policy for ICT before using any school ICT resource. New staff and students will be given a copy to read and sign. All signed forms will be kept in the office.

- The school will maintain a current record of all staff and pupils who are granted access to school ICT systems.

- Any person not directly employed by the school will be asked to sign an acceptable use of school ICT resources before being allowed to access the internet from the school site.

- Our school does not have any access to the school Wifi password and therefore we cannot grant access for visitors to the internet from any devices outside of NPT eg- personal computers and IPads. Visitors will have to use their own hotspot if they require internet access.

Assessing risks

- 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 NPTCBC can accept liability for any material accessed, or any consequences of Internet access.

- The school will 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.

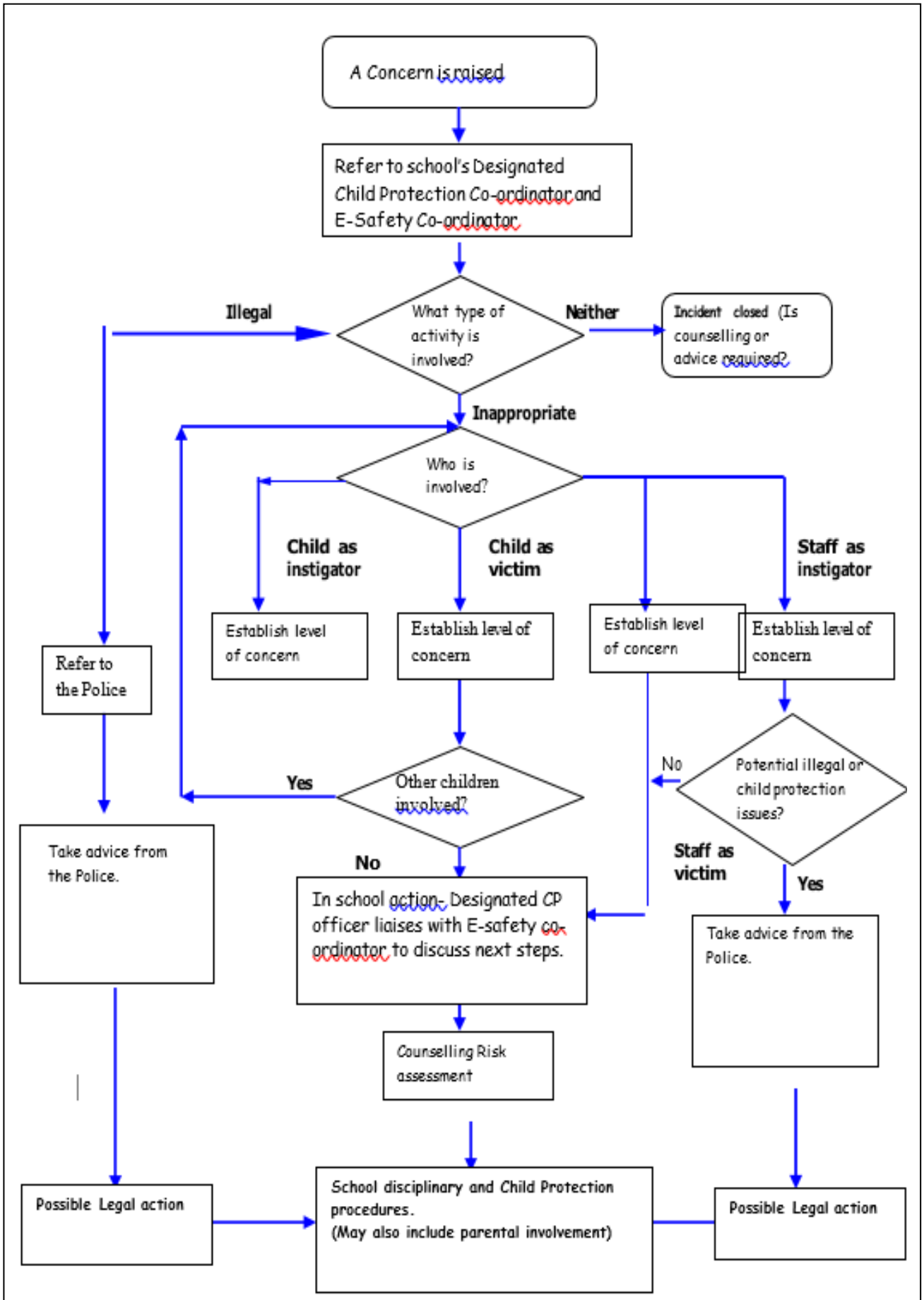
Handling e-safety complaints

- Complaints of Internet misuse will be dealt with by a senior member of staff following the school complaints procedure.
- 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.
- Pupils and parents will be informed of the complaints procedure.
- Pupils and parents will be informed of consequences for pupils misusing the Internet.
- Discussions will be held with the Community Police Officer to establish procedures for handling potentially illegal issues.

The Safeguarding Officer or E-Safety Coordinator can provide guidance should you be concerned about Internet use by a child, young person or member of staff.

The flowchart on the next page 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.

Reporting to an Incident of Concern



Community use of the Internet

- The school will liaise with local organisations to establish a common approach to E-Safety.

5. Communications Policy

Introducing the e-safety policy to pupils

- E-Safety rules will be posted in all rooms where computers are used and discussed with pupils regularly.
- Pupils will be informed that network and Internet use will be monitored and appropriately followed up.
- A programme of training in E-Safety will be developed.
  - E-Safety training will be embedded and incorporated into our school planning documents.

Staff and the e-Safety policy

- 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 that manage filtering systems or monitor ICT use will be supervised by senior management and work to clear procedures for reporting issues.
  - Staff will always use a child friendly safe search engine when accessing the web with pupils.

Enlisting parents' and carers' support

- Parents' and carers' attention will be drawn to the School e-Safety Policy in Newsletters, the school prospectus 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 agreement when they register their child with the school.