Abbey Primary School
Ysgol Gynradd Abbey

LA Esafety Policy

March 2025

Rights Respecting Children *Article 28 – The Right to Education*

Introduction

Abbey Primary School Esafety Policy is based on the Neath Port Talbot County Borough Council (NPTCBC) e-Safety Policy Guidance available on Digital Desk and Neath Port Talbot Learning Gateway (NPTLG) which 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 Becta and the Child Exploitation Online Protection (CEOP).

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

CONTENTS

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.

Further Information

- BITC Service Desk 01639 686767

1. E-Safety Audit – Primary / Special

Has the school an e-Safety Policy that complies with NPT guidance?	**Y**
Date of latest update (at least annual): March 2025	
The school e-safety policy was agreed by governors on: March 2025	
The policy is available for staff at: School Office	
The policy is available for parents/carers at: School Office	
The responsible member of the Senior Leadership Team is: Mr. K. Hodder	
The responsible member of the Governing Body is: Cllr. M. Harvey	
The Designated Child Protection Coordinator is: Mr. K. Hodder	
The e-Safety Coordinator is: Mrs. S Powell	
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 CEOP and Becta been obtained?	**Y**
Do all staff sign an Acceptable Use Policy for ICT on appointment?	**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**
Do parents/carers sign and return an agreement that their child will comply with the school e-Safety Rules?	**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**

2. School e-safety policy

The e-Safety Policy is part of the School Development Plan and relates to other policies including those for ICT, bullying and for child protection.

- The school has appointed an e-Safety Coordinator Mrs. S. Powell. The School Designated Child Protection Officer is Mr. Kevin Hodder.
- 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.
- The e-Safety Policy was revised by: Anthea Jackson
- It was approved by the Governors on: 12.03.25
- The next review date is (at least annually): March 2026

3.1 Teaching and learning

3.2.1 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.

3.2.2 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

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

3.2.4 Pupils will be taught how to evaluate Internet content

- The school will ensure that the use of Internet derived materials 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 e.g. using the CEOP Report Abuse icon or Hector Protector.

3.2 Managing Information Systems

3.3.1 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.

3.3.2 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.
- In e-mail communication, pupils must not reveal their personal details or those of others or arrange to meet anyone without specific permission.
- 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.

3.3.3 Published content and the school web site

- Staff or pupil personal contact information will not be published. The contact details given online should be the school office.
- The Head Teacher and E Safety Co-ordinator will take overall editorial responsibility and ensure that content is accurate and appropriate.

3.3.4 Publishing pupil's images and work

- Photographs that include pupils will be selected carefully so that individual pupils cannot be identified or their image misused. School will consider using group photographs rather than full-face photos of individual children.
- Pupils' full names will not be used anywhere on a school Web site or other on-line space, particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school Web site.
- Work can only be published with the permission of the pupil and parents/carers.
    - Pupil image file names will not refer to the pupil by name.
    - Parents should be clearly informed of the school policy on image taking and publishing, both on school and independent electronic repositories.

3.3.5 Social networking and personal publishing

- No social networking sites are allowed.

3.3.6 Managing filtering

- The school will work with the LLAN ICT sub-group to ensure systems to protect pupils are reviewed and improved.
- If staff or pupils come across unsuitable on-line materials, the site must be reported to the e-Safety Coordinator.
    - Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

3.3.7 Managing videoconferencing & webcam use

- Videoconferencing should use the educational broadband network to ensure quality of service and security.
- Pupils must ask permission from the supervising teacher before making or answering a videoconference call.
- Videoconferencing and webcam use will be appropriately supervised for the pupils' age.

3.3.8 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 are allowed on school premises under certain circumstances.
- 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.

3.3.9 Protecting personal data

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

3.3 Policy Decisions

3.4.1 Authorising Internet Access

- All staff must read and sign the Acceptable Use Policy for ICT before using any school ICT resource.
- The school will maintain a current record of all staff and pupils who are granted access to school ICT systems.
  - Parents will be asked to sign and return a consent form.
  - 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.

3.4.2 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.

3.4.3 Handling e-safety complaints

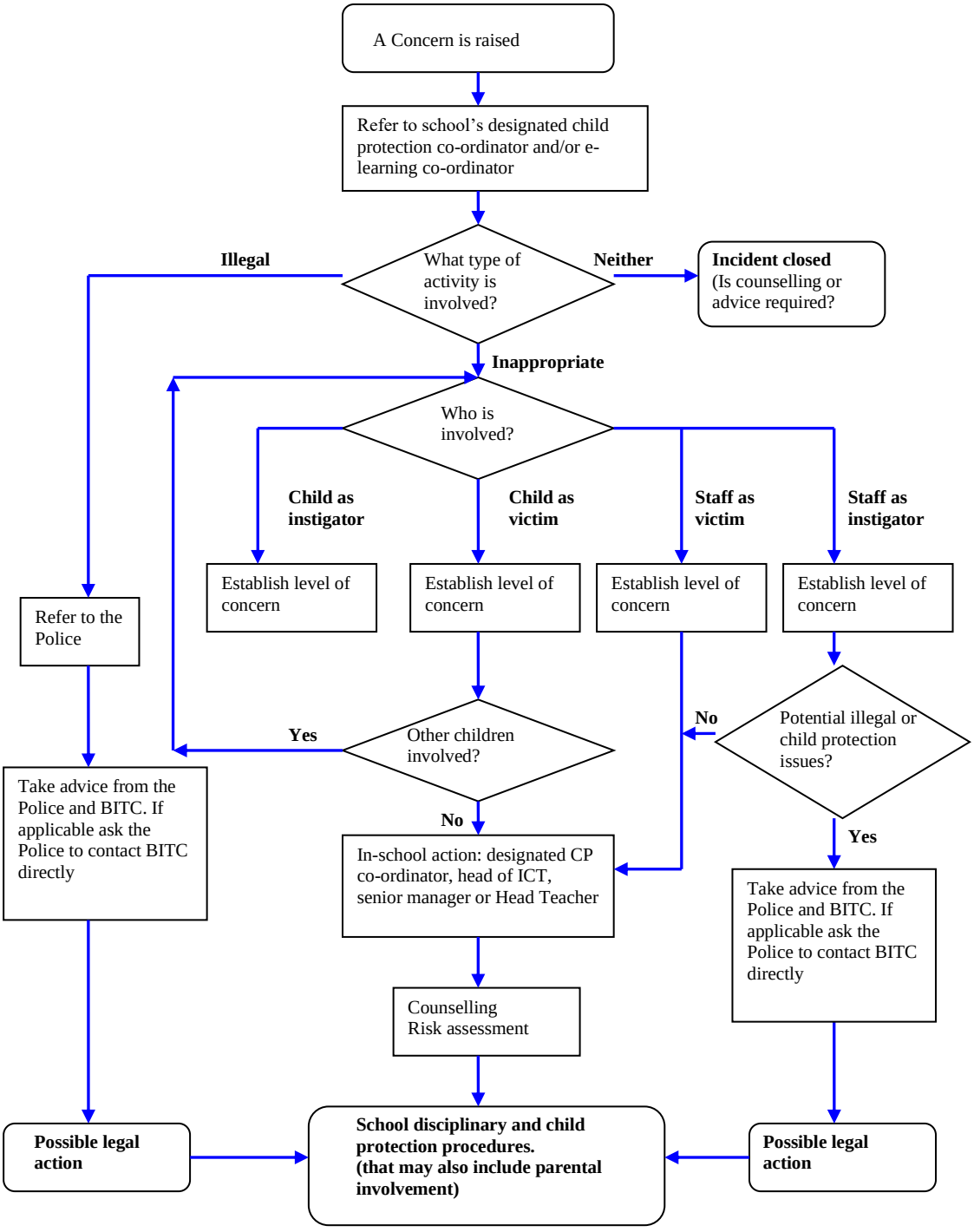
- Complaints of Internet misuse will be dealt with by a senior member of staff.
- Any complaint about staff misuse must be referred to the Head Teacher.
  - Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.

- Pupils and parents will be informed of the complaint's 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 the 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.

Response to an Incident of Concern



3.4.4 Community use of the Internet

- The school will liaise with local organisations to establish a common approach to e-safety.

3.4 Communications Policy

3.5.1 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 within the ICT scheme of work and/or the Personal Social Education (PSE) curriculum.

3.5.2 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.

3.5.3 Enlisting parents' and carers' support

- 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 agreement when they register their child with the school.

Appendices

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. Pupils should be supervised. Pupils 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. Pupils should be supervised. Pupils should be taught what internet use is acceptable and what to do if they access material they are uncomfortable with.
Exchanging information with other pupils and asking questions of experts via e-mail or blogs.	Pupils should only use approved e-mail accounts or blogs. Pupils should never give out personal information. Consider using systems that provide online moderation e.g. Superclubs Plus.
Publishing pupils' work on school and other websites.	Pupil and parental consent should be sought prior to publication. Pupils' full names and other personal information should be omitted. Pupils' work should only be published on 'moderated sites'.
Publishing images including photographs of pupils.	Parental consent for publication of photographs should be sought. Photographs should not enable individual pupils 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 blocked. Pupils should never give out personal information.
Audio and video conferencing to gather information and share pupils' work.	Pupils should be supervised. Schools should only use applications that are managed by Local Authorities and approved Educational Suppliers.

Appendix 2: Useful resources for teachers

BBC Stay Safe
www.bbc.co.uk/cbbc/help/safesurfing/
Becta
http://schools.becta.org.uk/index.php?section=is
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/
Kent Police – e-Safety
www.kent.police.uk/Advice/Internet%20Safety/e-safety%20for%20teacher.html
Think U Know
www.thinkuknow.co.uk/
Safer Children in the Digital World www.dfes.gov.uk/byronreview/

Appendix 3: Useful resources for parents

Care for the family
www.careforthefamily.org.uk/pdf/supportnet/InternetSafety.pdf
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
Parents Centre
www.parentscentre.gov.uk
Internet Safety Zone
www.internetsafetyzone.com