YSGOL CYBI

E-SAFETY Policy
Sept 2022

About this policy

The purpose of this policy is to highlight the importance of e-safety at school and how staff can implement all procedures and policies to ensure all children are safe when using the internet.

Date of next review	
This policy will be reviewed in:	September 2024
The review will be undertaken by:	Rhian Grieves

E-safety policy

YSGOL CYBI

CONTENT

1.1 What is e-safety?
1.2 Routes to e-safety
2.1 Who will create the policy?
2.2 Teaching and Learning
- 2.2.1 Why is using the Internet important?
- 2.2.2 How does using the Internet benefit education?
- 2.2.3 How can using the Internet enhance learning?
- 2.2.4 How do pupils learn how to evaluate content?

2.3 Regulating Information Services
- 2.3.1 How is the safety of information systems maintained?
- 2.3.2 How is e-mail regulated?
- 2.3.3 How is published content regulated?
- 2.3.4 Can the work or photos of pupils be published?
- 2.3.5 How is social networking and personal publishing regulated?
- 2.3.6 How is filtering software regulated?
- 2.3.7 How is videoconferencing regulated?
- 2.3.8 How can the latest technology be regulated?
- 2.3.9 How is personal data protected?

2.4 Policy decisions
- 2.4.1 How is access to the Internet authorised?
- 2.4.2 How is risk assessed?
- 2.4.3 How are complaints dealt with?
- 2.4.4 How is the Internet used across the community?

2.5 Communication Policy
- 2.5.1 How is the policy presented to the pupils?
- 2.5.2 How is the policy discussed with staff?
- 2.5.3 How is parental consent obtained?

3.0 Contact names and addresses in relation to e-Safety
4.0 Legal Framework

1.1 What is e-safety?

E-safety involves not only Internet technology but also electronic forms of communication such as mobile phones and wireless technology. It demonstrates the necessity to educate children and young people about the advantages, risks and responsibilities involved in using information technology. E-safety establishes safeguards and encourages awareness, ensuring that users manage their online experiences in a safe and positive manner.

The Internet is an open communication channel which anyone is free to use. The World Wide Web, e-mail, blogs and social networking can all transmit information around the world by way of the Internet at very little cost. Anyone can sent messages, discuss ideas and publish material with few restrictions. This makes the Internet an invaluable resource that is used by millions of people every day.

Much of the material found on the Internet is published for adults, and some of it is inappropriate for children. Information can also be found about weapons, crime and racism, and this is the easiest way to access such information. Pupils also need to learn that publishing personal material can endanger their personal safety and the safety of others.

1.2 Routes to e-safety

Safe and effective use of the Internet is now an essential life skill for pupils and staff alike. Unregulated access to the Internet can place pupils in an awkward, inappropriate and even dangerous situation. Schools must create and implement a policy that ensures that ICT is used responsibly, ensuring the safety of pupils, by consulting staff, parents, governors and the education authority. The e-Safety policy will complement other policies, including Behaviour, Anti-Bullying and the Curriculum.

Electronic communication between staff and pupils

Staff and pupils must understand that using the school network is a privilege that can be removed at any time if there is sufficient reason for doing so. The school is able to monitor all use of the network and Internet to ensure the safety of pupils through the LEA.

Every user is expected to follow rules of etiquette (net-etiquette) when using the network. These include the following:

- Be polite.
- Use appropriate language.
- Do not use offensive language when communicating with others.
- Do not reveal your address, phone number or any other details about yourself or others.
- Do not use the internet in a way that interferes with the way in which others are using the network.
- Illegal activities are forbidden.
- It cannot be guaranteed that an e-mail will be private.
- The system managers monitor and can access every e-mail.
- Messages that relate to illegal activities or that support such activities will be brought to the attention of the authorities.

Use of new technology in education

New technologies should be investigated in order to assess their educational benefit, and a risk assessment must be made before permission is granted to use the technology in the school. Secondary schools (and in particular their pupils) are leading

the way in the use made of a wide variety of new technologies and learning opportunities, including:

- Mobile phones powered by computer which can be connected to the Internet, Bluetooth and infrared camera.
- New learning environments such as Moodle and other learning platforms
- Thinking skills that are challenged by games and simulations
- Internet voice messaging such as Skype and IWB link.
- Digital storytelling which involves independent thinking and self-motivation
- Podcasting, broadcasting and recording lessons
- Digital video

Some of these technologies may disappear. Others will evolve. What matters is combining the ability of young people to experiment with the wisdom of teachers in order to develop the appropriate, effective and safe use of technology in teaching and learning.

1.3 Responding to an incident that causes concern

Internet technology and electronic communication provides children and young people with the opportunity to broaden their experiences and develops their creative ability within school and beyond. However, it is important to be aware of the dangers of using these technologies.

The risks to e-safety occur because of people who act inappropriately or even illegally. Any personal matter that arises must be dealt with. Teachers are the front line of defence; it is they who observe the pupils, and this is crucial with regard to becoming aware of risks to pupils and gaining the trust of pupils so that matters can be dealt with. Incidents can vary from a thoughtless action or piece of mischief to illegal action that has been carefully planned.

What does electronic communication include?

- **Ways of interacting on the Internet:** social networking sites and web-logs (blogs)
- **Internet research**: websites, search engines and web browsers
- **Mobile phones and personal digital aids** (PDAs)
- **Communicating via the Internet:** e-mail and instant messaging
- **Webcams and video conferencing**
- **Wireless games consoles**

What are the dangers?

- Receiving inappropriate content
- Grooming and cultivating an inappropriate relationship
- Requests for personal information
- Viewing sites that 'encourage'
- Bullying and threats
- Identity theft
- Publication of inappropriate content
- Online gambling
- Abuse of computer systems
- Publication of personal information
- Hacking and breaking safety rules
- Corrupting or misusing data

How should we respond?

The Child Protection Safety Officer can provide guidance when a member of staff is concerned about the use made of the Internet by a child, young person or member of staff.

The flowchart on the last page shows the steps that must be taken when dealing with a matter of concern. This diagram should only be a starting point, as the Department

for Education and Children's Services provide additional documents to help schools respond to incidents which involve child safety. County and School policies for Child Safety can be consulted.

2.1 Who will create and review the policy?

- The school will appoint a specific member of staff who will be responsible for e-Safety / ICT.
- The e-Safety Policy will be implemented and reviewed every two years.
- The e-Safety Policy has been written by the school, based on Anglesey Council's e-Safety Policy and government guidelines. The school's senior managers have agreed on the policy and the school's governors have approved it.

2.2 Teaching and learning

2.2.1 Why is using the Internet important?

- The purpose of using the Internet in school is to raise educational standards, facilitate pupil attainment, support the professional work of staff and improve the school's managerial functions
- Using the Internet is part of the statutory curriculum and an essential tool for learning.
- Internet access is one of the rights of pupils who demonstrate a responsible and mature attitude towards use of the media.
- The Internet is an essential element of life in the twenty-first century in relation to education, business and social links. It is the school's duty to provide pupils with easy access to the Internet as part of their learning experience.
- Pupils make extensive use of the Internet outside school, and need to learn how to evaluate the information on the web and be responsible for their own safety.

2.2.2 How does using the Internet benefit education?

The following are some of the benefits of using the Internet in education:

- access to global resources including museums and art galleries;
- being a part of the Welsh Lifelong Learning Network which links every school in Wales;
- educational and cultural exchanges between pupils across the world;
- vocational, social and leisure resources in libraries, clubs and at home;
- access for pupils and staff to expertise in many areas;
- professional development for staff who can access national developments, educational resources and effective practice for teaching the curriculum;
- co-operation across the support services and professional organisations;
- better access to technical support, including remote control of networks and automatic updates for systems;
- exchanging curriculum and administrative data with the Authority and the Assembly;
- access to learning wherever and whenever it's convenient.

2.2.3 How can using the Internet enhance learning?

- Access to the Internet will be designes specifically for the use of pupils, and will include a filtering system which is appropriate for the age of pupils.
- Staff should give guidance to pupils about online activities that will support learning outcomes planned according to the age and maturity of the pupils.

- Pupils receive guidance on acceptable and unacceptable use of the Internet, and are given clear objectives when using the Internet.
- Access to the Internet is planned with a view to enhancing and extending learning activities. Access levels will be revised according to curriculum requirement and the age of pupils.
- Pupils will be taught to use the Internet effectively in research work, including skills that allow them to find, retrieve and evaluate information.

2.2.4 How do pupils learn how to evaluate Internet content?

- Schools will ensure that materials obtained from the Internet that are copied or used on other occasions by staff and pupils conform to copyright law.
- Pupils should be taught to be critically aware of the materials they read, and should be shown how to verify information before accepting it as accurate.
- Pupils will be taught to acknowledge the source of the information they are using and to respect copyright when using Internet materials in their work.

2.3 Managing Information Systems

2.3.1 How is the safety of information systems maintained?

- The safety of school information systems are regularly reviewed.
- Anti-virus protection is regularly updated and managed by the LEA
- Reserve strategies (including offline and offsite requirements) will be considered and will correspond with school requirements with regard to retrieval in the event of a disaster.
- Safety strategies will be discussed with Anglesey County Council where appropriate.
- Personal data sent over the Internet will be encrypted or made safe by other means.
- No portable device may be used without specific permission and being subjected to an examination for viruses.
- Permission will not be given for system facilities that have not been approved or files that can be activated within the work of pupils or sent by e-mail.
- Files that are kept on the school network are regularly scrutinised.
- The ICT co-ordinator / network manager will review the system's capacity regularly.

2.3.2 How is e-mail regulated?

- Pupils may only use e-mail accounts approved by the school.
- Pupils must inform a teacher immediately if they receive an offensive e-mail.
- Pupils must not reveal personal details about themselves or others in an e-mail message, or arrange to meet anyone without specific consent.
- Overuse of social e-mailing can hamper learning, and restrictions are therefore in place.
- Care should be taken when e-mailing outside establishments and permission should be sought before sending an e-mail, as with letters written on headed notepaper.
- Permission will not be given to send chain letters on to other addresses.

2.3.3 How is published content regulated?

- The school's address, e-mail address and phone number should be included as contact details on the website. Personal information about staff or pupils must not be published.

- The SLT and administrative team will be responsible in general for editing the material and ensuring that it is accurate and appropriate.
- Care should be taken when publishing e-mail addresses to avoid receiving spam.
- The website / social networks should correspond with school guidelines for publications, including respect for intellectual property and copyright.

2.3.4 Can the work or photos of pupils be published?

- Photos which include pupils are chosen carefully. Text which accompanies pictures should not identify individual pupils.
- Pupil names are not used anywhere on the website in connection with photographs.
- Written approval is sought from parents before photos of pupils are included on the website.
- Work can only be published with the consent of the pupil and his/her parents.

2.3.5 How is social networking and personal publishing regulated?

- The school will block / filter access to social networking sites. (Anglesey County filtering service currently blocks access to a number of social networking sites. However, schools are responsible for giving information about any other sites they may need to filter /block).
- Inappropriate forums will be blocked.
- Pupils are advised never to give out any personal details that give information about their identity or location. Examples include real name, address, mobile phone number or house number, school attended, IM and e-mail addresses, full names of friends, specific interests and clubs etc.
- Pupils should be told not to include personal photos on any social network space. They should consider how public the information may be, and consider using private areas. Advice should be given about any background details in the photo that might identify the pupil or his / her location e.g. house number, street name or school.
- Passwords should be used to safeguard blogs or official wikis made by teachers, and these should be run on the school website. Teachers should be advised not to run social networking spaces for the personal use of pupils.
- Pupils should be advised about safety and encouraged to create passwords, refuse access to individuals they do not know, and be trained on how to prevent unwelcome messages. Pupils should be encouraged to invite only friends, and to refuse access to others.
- Pupils should be advised to refrain from publishing specific, detailed private thoughts.
- Schools should be aware that bullying can occur through social networking, in particular where a space has been created which is unprotected by a password and others have been invited to view the bully's comments.

2.3.6 How is filtering regulated?

- The school will work with Anglesey County Council, taking Becta guidelines into consideration, to ensure that systems that protect pupils are regularly revised and improved.
- If staff or pupils discover inappropriate websites, the URL must be given to the e-Safety / ICT Co-ordinator and systems manager, to be forwarded immediately to Anglesey Council IT Services helpdesk and distributed to every school system.
  All access to the Internet in school will be logged.

- Internet use will be randomly monitored to ensure that it conforms with school policy.
- All Internet access within the school is filtered. Under rare circumstances, there will be a genuine need to bypass technical restrictions by using an unfiltered connection. The Headteacher should give personal permission every time the Internet is used without a filter, and review the need for regular access.
- The school uses a combination of Walled Garden access and Filtered access which is appropriate for the age of pupils, to support pedagogical objectives.
- The school's e-Safety policy is compatible with the school's policy with regard to discipline.
- Senior members of staff will ensure that filtering methods are regularly reviewed to ensure that those methods are appropriate, effective and reasonable.
- The appropriate agencies must be informed about any material that the school believes to be illegal.
- Educationalists will create the school's filtering strategy according to the age and curricular requirements of pupils, and the advice of Anglesey County IT technicians and Advisers.

2.3.7 How is videoconferencing monitored?

- The school uses Microsoft TEAMS (Hwb) to hold online lessons with groups if and when required.
- All videoconferencing equipment in class should be switched off when not in use.
- Equipment that is connected to Lifelong Learning Wales Network use the national E.164 numbering system.
- External IP addresses should not be made available to other sites.
- Videoconferencing contact information should not be included on the school website.
- The equipment must be kept safe and locked up if necessary when not in use.
- Videoconferencing equipment should not be taken away from the school campus without permission. The way a network is used cannot be monitored or controlled on any network apart from the educational network.

Users

- Pupils should seek the permission of the supervising teacher before making or answering a videoconferencing call.
- Videoconferencing should be appropriately supervised according to the age of the pupils.
- The agreement of parents and guardians should be sought when children take part in videoconferences.
- Great care must be taken when delegating responsibility for the use of videoconferencing equipment outside school hours.
- Only key members of staff should have access to the videoconferencing system, website or other remote control page which is available on larger systems.
- Only members of staff should have access to any unique logon details and passwords for the educational videoconferencing services, and these details should be kept in a safe place.

Content

- When recording a videoconferencing lesson, every site and everyone who takes part should give their written permission. The reason for the recording must be given and at the start of the conference it should be made clear to all who take part that the conference is being recorded.
- Material that is being recorded must be stored safely.
- If material belonging to a third party is included, ensure that making a recording is acceptable to avoid transgressing the intellectual property rights of the third party.
- Videoconferencing is a challenging activity that provides pupils with a wide variety of learning benefits. Preparation and evaluation are essential parts of the whole activity.
- Dialogue should be held with others who are involved in the conference before taking part in the videoconference. If the conference is taking place on a different site, away from the school, it is important that it provides material that is appropriate for your class.

2.3.8. How can the latest technology be regulated?

- The latest technologies will be examined for their educational value, and a risk assessment will be made before permission is granted to use them in the school.
- Mobile phones must not be used during lessons or formal lesson time. Abusive or inappropriate text messages are banned.
- The school must investigate infrared link and Bluetooth technologies and create a policy for their use in the school.

2.3.9 How is personal data protected?

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

2.4 Policy Decisions

2.4.1. How is access to the Internet authorised?

- The school will keep an ongoing record of every staff member and pupil who has permission to access the school's electronic links.
- Pupils must apply individually for access to the Internet by agreeing to conform to the e-Safety Rules.
- Parents are asked to sign and return a form granting permission for pupils to access the Internet.
- Parents are informed that pupils will be granted access to the Internet under supervision.

2.4.2 How is risk assessed?

- The school will take every reasonable step to ensure that users have access to appropriate material only. Despite this, because of the global nature of the Internet and its subject links, it is impossible to guarantee that inappropriate material will never be accessed on a school computer. Neither the school nor Anglesey County Council can accept responsibility for the material that is accessed or for any consequences that may result from use of the Internet.
- The school should examine the use made of ICT to discover if its e-safety policy is adequate and ensure that the e-safety policy is being appropriately implemented.
- Using computer systems without permission or for inappropriate purposes can be a crime under the Computer Misuse Act 1990.

- The methods of recognising, assessing and reducing the risks are regularly reviewed.

2.4.3 How are complaints about e-safety dealt with?

- A senior member of staff deals with complaints about misuse of the Internet.
- Any complaints about staff misusing the Internet must be directed to the Headteacher.
- Pupils and parents are informed about the complaints procedure.
- Parents and pupils must work in partnership with staff to resolve matters.
- Discussions are held with the local Police Public Protection Unit to establish procedures for dealing with possible crimes.
- The punishments cited in the school's policy include the following:
- interview/counselling from the head of year;
- informing parents and guardians;
- banning access to the Internet or a computer for a specific period of time.

2.4.4 How is the Internet used across the community?

- The school will contact local organisations to ensure that there is a common approach towards e-safety.
- The school will demonstrate sensitivity when dealing with matters involving the Internet that pupils discover outside school, e.g. social networking sites, and offer appropriate advice.

2.5 Communication Policy

2.5.1 How is the policy presented to the pupils?

- E-safety rules will be displayed in rooms that have Internet access.
- Pupils are made aware that all use of the Internet is monitored.
- An e-safety programme is presented to raise awareness of the importance of using the Internet safely and responsibly.
- Guidelines should be given on how to use the Internet responsibly and safely before allowing access to the Internet.
- A module on e-safety will be included in the RSE/ICT programmes that encompass use of the Internet in the school and at home.
- The school police liason officer will work with pupils to present a unit of work on internet safety at the beginning of each term.
- HWB Cymru- allows access to pupils to gain information on E-safety.

2.5.2 How is the policy discussed with staff?

- Every member of staff receives a copy of the school's E-safety Policy and an explanation of how to implement the policy and the importance of the policy.
- Staff should be aware that Internet traffic can be monitored and tracked. Acting wisely and behaving in a professional manner is of the utmost importance.
- Staff who manage the filtering systems or monitor the use of ICT are supervised by senior managers, and have clear procedures for reporting any matters of concern(LEA)
- Training is provided on how to use the Internet safely and responsibly and on the school's E-safety Policy whenever necessary.

2.5.3 How is parental consent obtained?

- Parents are made aware of the school's Policy by means the school admission handbook and the school website.
- Matters relating to the Internet are treated with sensitivity, and parents are informed of any steps that have been taken.
- Working in partnership with parents is encouraged. This can include parents' evenings that include displays and suggestions on how to use the Internet safely at home.
- Parents are given advice about filtering systems and educational and leisure activities which include using the Internet.
- Parents who are interested are directed to the organisations listed in section 3.0, E-safety Contact Names and Addresses.
- Parents are invited to E-Safety talks with the police liason officer once a year.
- Parents are offered advice via class dojo relating to internet safety issues.

3.0 E-safety Contact Names and Addresses

Child Exploitation & Online Protection Centre
http://www.ceop.gov.uk
Think U Know website
http://www.thinkuknow.co.uk/
Wise Kids website
www.wisekids.org.uk
Internet Watch Foundation
http://www.iwf.org.uk/
Childline
http://www.childline.org.uk/
BBC Chat Guide
http://www.bbc.co.uk/chatguide/
Internet Safety Zone
http://www.internetsafetyzone.com/
Kidsmart
http://www.kidsmart.org.uk/
NCH – The Children's Charity
http://www.nch.org.uk/information/index.php?i=209
NSPCC
http://www.nspcc.org.uk/html/home/needadvice/needadvice.htm
Stop Text Bully

www.stoptextbully.com
Virtual Global Taskforce – Report Abuse
http://www.virtualglobaltaskforce.com/

4.0 The Legal Framework

Notes on the legal framework

Many young people and even members of staff regularly use the Internet without realising that some of the activities they are doing are possibly illegal. The law develops rapidly and recent changes have been enforced by means of the following:

- The Sexual Offences Act 2003, which deals with new offences such as fostering an inappropriate relationship online, and making/distributing indecent images of children, has raised the age of a child to 18;
- The Racial and Religious Hatred Act 2006 which creates new offences involving incitement of hatred based on religious belief; and
- The Police and Justice Act 2006 which extends the limits of the Misuse of Computers Act by criminalising failing to prevent an attack on the system.

Racial and Religious Hatred Act 2006
This Act criminalises the act of threatening people because of their religious beliefs, or inciting religious hatred by showing, publishing or distributing written material that is threatening. Other laws already protect people agains threats based on race, gender or ethnic background.

Sexual Offences Act 2003
The new offence of cultivating an inappropriate relationship online is committed is you are 18 years old and have communicated with a child of under 16 years of age at least twice (including by phone or over the Internet). It is an offence to meet them or to travel to meet them anywhere in the world with the intention of committing a sexual offence.

Forcing a child of under 16 years of age to watch a sexual act, including looking at videos, photographs or a web camera, for your own pleasure is illegal..

It is also an offence for a person in a position of trust to commit a sexual act with any person under 18 years of age over whom they have a position of trust. (Teachers, social workers, your workers and health professionals are all included in this category of trust).

Anyone who has sexual intercourse with a child of under 13 years of age is committing rape.

N.B. Schools may already possess a copy of "*Children & Families: Safer from Sexual Crime*" as part of their child safety package.

More information about the 20?? Act can be found on www.teachernet.gov.uk

Communications Act 2003 (section 127)
Sending a message or other content that is extremely offensive or of an indecent, obscene or threatening nature via the Internet; or sending false messages via the Internet or using the Internet constantly to unnecessarily anger, inconvenience or worry someone, is guilty of a crime that may lead to a period in prison.

This wording is important as an offence has been committed as soon as the message has been sent: it is not necessary to prove any intent or purpose.
Data Protection Act 2018
This Act requires that anyone who deals with personal information should inform to the Information Commissioner's Office about the type of processing they are

undertaking, and they must conform to important principles of data protection when dealing with personal data relating to a living person. The Act also grants individuals the right to see the personal information relating to them that is being held, receive compensation and prevent processing of the information.

Misuse of Computers Act 1990 (sections 1 – 3)

Irrespective of the individual's motive, the Act dictates that it is a crime to:

- Access computer files or software without permission (e.g. using someone else's password to gain access to files);
- Access without permission, as above, in order to commit another offence (such as deception); or
- Interfere with a computer or programme's ability to function (for example caused by a virus or by failing to prevent an attack on the system).

UK citizens or residents can be extradited to another country if it is suspected that they have committed one of the above offences.

Malicious Communications Act 1988 (section 1)

This legislation dictates that it is a crime to send an electronic message (e-mail) that conveys indecent, extremely offensive, threatening or untrue information; or that is of an indecent nature or extremely offensive if the intention was to cause the recipient concern or anxiety.

Copyright, Designs and Patents Act 1988

Copyright is an individual's right to prevent others from copying or using his or her "work" without permission.

The material under copyright (known as "work") must be a work that was created by the author themselves and the product of skill and judgement. Copyright arises when an individual expresses an idea in a tangible form. Works such as text, music, sound, film and programmes are all eligible for protection by copyright. It is usually the author of the work who owns the copyright, but if the work was created during employment, then it is the employer who owns the copyright.

Making a copy of the whole or a substantial part of anyone's work without the author's permission is an infringement of copyright. There will usually be a certificate accompanying the work that permits the user to copy or use it for restricted purposes. It is always wise to read the terms of the license before making a copy or using anyone else's material.

It is also illegal to adapt or use software without a license or in any way that is prohibited by the conditions of the software license.

Public Order Act (sections 17 – 29)

This Act dictates that it is an offence to incite racial hatred by showing, publishing or distributing written material that is threatening. As in the case of the Racial and Religious Hatred Act, it is also an offence to be in possession of inflammatory material with the intention of releasing it.

Child Protection Act 2016 (Section 1)

It is an offence to take, give permission to take, make, possess, show, distribute or advertise indecent photographs of children in Great Britain. In this case, a child means anyone under 18 years of age. Looking at an image of a child on your computer means that you have made a digital image. An image of a child also includes making false images (digitally altered or otherwise). A person who is found guilty of such a crime could face a period of 10 years in jail.

Obscene Publications Act 1959

Publishing an “obscene” article is a crime. Publishing includes electronic transfer.

Protection from Harrassment Act 1997

A person must not behave in a manner that causes harassment to another person, when he or she knows, or should know, that the behaviour is causing harassment. A person behaving in a manner that causes another person, on at least two occasions, to believe that violence will be inflicted on them, is guilty of an offence if they know or should know that their behaviour is causing another person fear.

Regulation of Investigatory Powers Act 2000

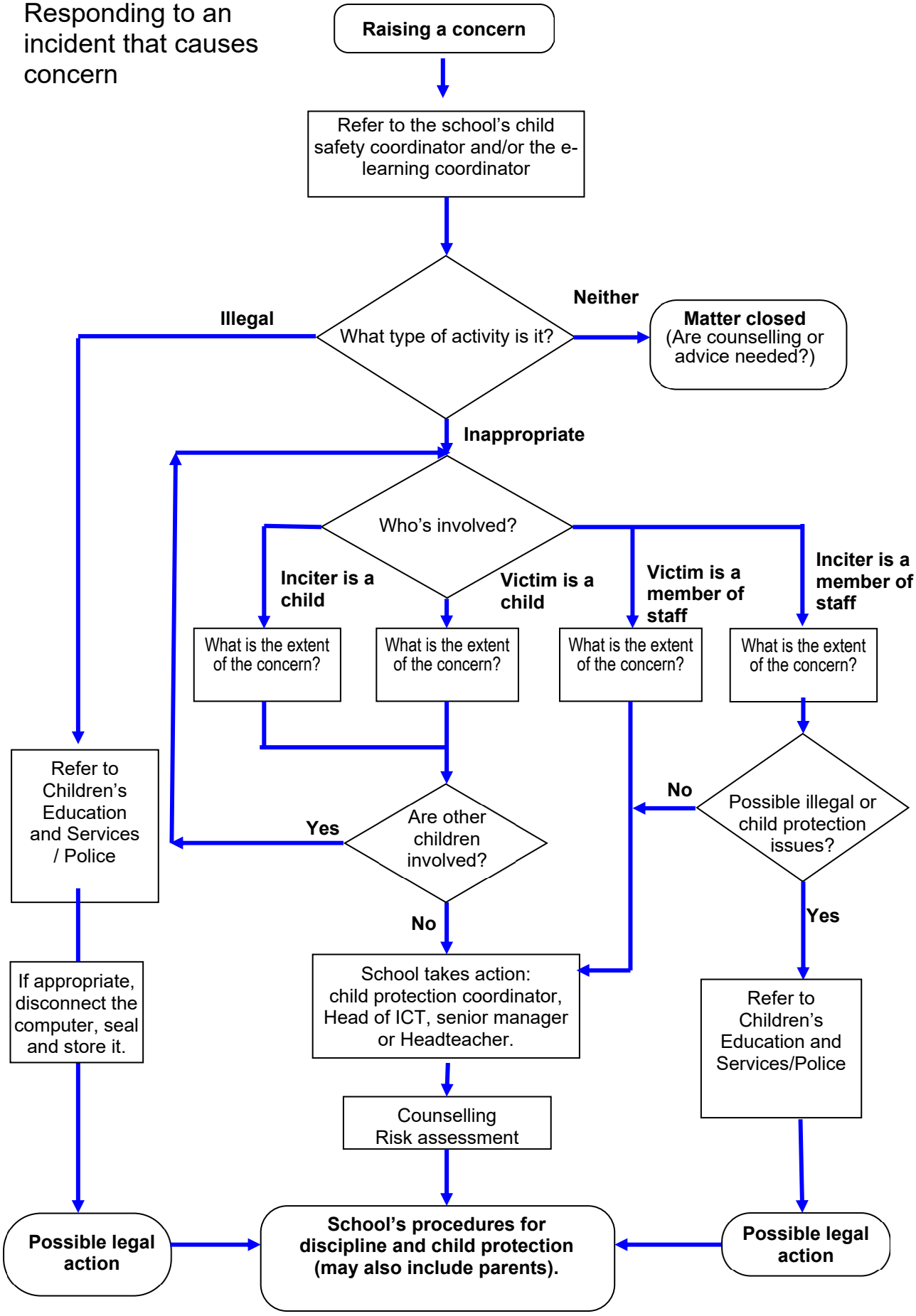
The Regulation of Investigatory Powers Act 2000 regulates the process of intercepting communications and makes it an offence to intercept or monitor communications without the permission of the parties who are involved in the communications. This Act was passed to conform with the Human Rights Act

Telecommunication Regulations (Lawful Business Practices)(Interception of Communications), however, permits a certain amount of monitoring and record keeping, for example, to ensure that the communication is relevant to a school’s activities or in order to investigate or discover use made of the internet without permission. Despite this, before monitoring, permission should be obtained based on information, which means that steps must be taken to ensure that everyone who is going to use the system knows that the communication is going to be monitored.

Secretly monitoring without informing the users that someone is doing so risks infringing data protection legislation and privacy legislation.

Cookie law

The Cookie Law is a piece of privacy legislation that requires websites to get consent from visitors to store or retrieve any information on a computer, smartphone or tablet.

http://www.cookielaw.org/the-cookie-law/

Responding to an incident that causes concern