# Caersws CP School E-Safety Policy

**Introduction**

The purpose of this policy is to ensure that all staff, parents, governors and children understand and agree the school's approach to e-safety. The policy relates to other policies including ICT Policy/ curriculum, Anti-Bullying, Child Protection, Safeguarding, Social Media and Health and Safety and Acceptable Use Policy (AUP.)

**Aims**

The Aims of this Policy are:

- To promote safe use of the internet by pupils at our School and at home.
- To enable the internet to be used safely and imaginatively at School to promote pupil achievement, to support the professional work of staff and to reinforce the School's management systems.
- To educate pupils about the risks of electronic social networking and on methods of safeguarding themselves and others from those risks.
- To support all members of the School community in complying with relevant legal requirements

**Reviewing the e-Safety policy**

**This policy will be reviewed annually due to the constant change in Information Technology.**

**Roles and Responsibilities**

The following section outlines the e-Safety roles and responsibilities of individuals and groups within the school:

**Governors:**

Governors are responsible for the approval of the e-Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the *Governor responsible for ICT* receiving regular information about e-Safety incidents and monitoring reports. This member of the Governing Body should take on the role of e-Safety Governor to include:

- *regular meetings with the e-Safety Co-coordinator / Officer*
- *reporting to the Governor body*

**Head teacher**

- The *Head teacher* has a duty of care for ensuring the safety (including e-Safety) of members of the school community.
- The Head teacher and SMT should be aware of the procedures to be followed in the event of a serious e-Safety allegation being made against a member of staff.
- Follow procedures set out in Online Incident flow chart (Appendix C)

**The *e-Safety Officer***

- leads the e-Safety committee and school council
- takes day to day responsibility for e-Safety issues and has a leading role in establishing and reviewing the school e-Safety policies / documents
- Ensures that all staff are aware of the procedures that need to be followed in the event of an e-Safety incident taking place.
- provides (or identifies sources of) training and advice for staff
- liaises with the Local Authority
- liaises with technical staff
- Receives reports of e-Safety incidents and creates a log of incidents to inform future e-Safety developments.
- meets regularly with e-Safety *Governor* to discuss current issues, review incident logs and if possible, filtering / change control logs
- attends relevant *Governor Body* meetings.

**Teaching and Support Staff**

Are responsible for ensuring that:

- they have an up to date awareness of e-Safety matters and of the current school e-Safety policy and practices
- they have read, understood and signed the Staff Acceptable Use Policy.
- they report any suspected misuse or problem to the *Headteacher / Deputy Head for* investigation and complete an Incident Log Form (Appendix B)
- all digital communications with students / pupils / parents / carers should be on a professional level.

**Safeguarding Designated Person**

The *Head Teacher* has had training in e-Safety issues and is aware of the potential for serious safeguarding issues to arise from:

- sharing of personal data
- access to illegal / inappropriate materials
- inappropriate on-line contact with adults / strangers
- potential or actual incidents of grooming
- cyber-bullying

**e-Safety Group**

The e-Safety Group provides a consultative group that has wide representation from the school community, with responsibility for issues regarding e-Safety and monitoring the e-Safety policy including the impact of initiatives. The group will also be responsible for regular reporting to the Governing Body. The group will meet once every half term.
The e-safety group will meet with the chair of Governors and make suggestions.

**Pupils:**

- are responsible for using the school digital technology systems in accordance with the Pupil Acceptable Use Policy
- have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- should understand the importance of adopting good e-Safety practice when using digital technologies out of school and realise that the school's e-Safety Policy covers their actions out of school, if related to their membership of the school.

**Parents / Carers**

Parents / Carers play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way. The school will take every opportunity to help parents understand these issues through *parents' evenings, newsletters, letters, website /literature.* Parents and carers will be encouraged to support the school in promoting good e-Safety practice and signing the school Parent Acceptable Use Policy

**Policy Statement: Education**
E-Safety should be a focus in all areas of the curriculum and staff should reinforce e-Safety messages across the curriculum. The e-Safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways:

- A planned e-Safety curriculum should be provided as part of ICT / Computing / PSE / Digital Literacy lessons.
- Pupils should be taught in all lessons to be critically aware of the materials / content they

access on-line and be guided to validate the accuracy of information.

- Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.

**Education & Training – Staff**

It is essential that all staff receive e-Safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- A planned programme of formal e-Safety training will be made available to staff. This will be regularly updated and reinforced.
- All new staff should receive e-Safety training as part of their induction programme, ensuring that they fully understand the school e-Safety policy and Acceptable Use Policy.
- All staff and volunteers are expected to sign the Acceptable Use Policy (for Staff and Volunteers- see appendix.)

**Bring Your Own Device (BYOD)**

No devices are allowed in school unless consent has been granted by the Head Teacher. Devices may be allowed in school from specialist services if they are to support the learning of pupils.

**Teaching and Learning**

**The importance of internet and digital communications**

The purpose of Internet access in school is to raise educational standards, to support the professional work of staff and to enhance the school's management information and business administration systems. Access to the Internet is a necessary tool for staff and learners. It helps to prepare learners for their on-going career and personal development needs. It is a requirement of the National Curriculum (NC) orders for ICT and is implied in other subject orders.

**Internet use enhances learning**

Internet access is provided by Powys County Council and designed for pupils. This includes filtering appropriate to the content and age of pupils. Internet access is planned to enrich and extend learning activities. Access levels are reviewed to reflect the curriculum requirement. Pupils are given clear objectives for Internet use and sign an Internet agreement. Staff selects sites which support the learning outcomes planned for pupils' age and maturity. Pupils are taught how to take responsibility for their own Internet access.

**Pupils are taught how to evaluate Internet content**

Pupils are taught ways to validate information before accepting that it is necessarily accurate. Pupils are taught to acknowledge the source of information, when using Internet material for their own use. Pupils are made aware that the writer of an e-mail or the author of a Web page might not be the person claimed. Pupils are encouraged to tell a teacher immediately if they encounter any material that makes them feel uncomfortable.

**Managing Internet Access**

**Information System Security**

School ICT system security is reviewed regularly.
Virus protection is updated regularly.
Security strategies are discussed with the Local Authority.

The School recognises that many children now engage in social networking (and/or personal publishing) at a surprisingly young age, that this presents significant safeguarding risks and that both parents/carers and the School should seek to safeguard pupils and educate them in self-protection.

**E-mail**

Pupils are allowed to use school e-mail accounts only. Pupils must tell a teacher immediately if they receive offensive e-mail. In e-mails, pupils are taught that they must not reveal their personal details,

those of others or arrange to meet anyone without specific permission. Pupils are taught not to open suspicious incoming e-mail or attachments. The forwarding of chain letters is not permitted.

**School Email Management Staff**
Staff who maintain personal email addresses at caersws.powys.sch.uk are responsible for appropriate management of them. Individual staff email addresses will for security protection reasons not be placed on the School website. Staff can be contacted via the "office@caersws" address which is open to all teaching staff or within school by designated email addresses.

**Social networking and personal publishing**
Pupils will not be allowed to access public chat rooms apart from Hwb+. New applications will be thoroughly tested before pupils are given access.

**Managing filtering**
The school works in partnership with parents, the LA, ERW, The National Assembly for Wales and the Internet Service Provider to ensure systems to protect pupils are reviewed and improved. As a rule, all internet access to the School system is filtered. Use of an unfiltered connection may occasionally be necessary, but requires the permission of the Head Teacher.
If staff or pupils find a site which appears unsuitable, information about that site with the URL must be reported to the Coordinator who will ensure that the details are reported to the PCC IT Helpdesk. Any internet material which staff believe to be illegal must be reported to the Coordinator who will consult the Head Teacher on reporting it to the appropriate agency. The responsibility for the management of the school's filtering policy will be held by The Head Teacher. They will manage the school filtering, in line with this policy and will keep records / logs of changes and of breaches of the filtering systems.

**Password Security**

A safe and secure username / password system is essential if the above is to be established and will apply to all school technical systems, including networks, devices, email and Virtual Learning Environment (VLE).

- All school networks and systems will be protected by secure passwords that are regularly changed
- The 'administrator' passwords for the school systems are available to the *Headteacher* and kept in a secure place (school office-password book.)
- Consideration should also be given to using two factor authentications for such accounts.

**Staff passwords:**

- All staff users will be provided with a username and password by *(the Head Teacher) who will keep an up to date record of users and their usernames.*

**Student / pupil passwords:**

- All users will be provided with a username and password by (*The Head Teacher) who will keep an up to date record of users and their usernames.*

**Managing video conferencing and webcam use**
Video conferencing is not yet available.

**Managing emerging technologies**
Only school cameras are used by both staff and children for educational purposes. Pupils are not currently permitted to bring mobile telephones, tablets, or similar electronic devices into school or on school trips. The School will keep under review (and risk assess) the use of emerging technologies by pupils in School. Cameras in mobile phones are not to be used by staff.

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

**Use of digital and video images**

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents / carers and students / pupils need to be aware of the risks associated with publishing digital images on the internet. All parents are asked to sign a Digital Media form which gives a clear mandate as to what images can be taken and shared with others. These forms are kept in the office.

**Data Protection**

**The school ensures that:**

- It will hold the minimum personal data necessary to enable it to perform its function and it will not hold it for longer than necessary for the purposes it was collected for.
- Every effort will be made to ensure that data held is accurate, up to date and that inaccuracies are corrected without unnecessary delay.
- All personal data will be fairly obtained in accordance with the "Privacy Notice" and lawfully processed in accordance with the "Conditions for Processing".
- Has a Data Protection Policy
- It is registered as a Data Controller for the purposes of the Data Protection Act

**Staff must ensure that they:**

- At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.
- Use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data.
- Transfer data using encryption and secure password protected devices.

**Policy Decisions**

**Authorising Internet access**

Parents are asked to sign a consent form regarding their child's internet use (see Acceptable Use Policy). Any person not directly employed by the school will be asked to read this e-safety policy.

**Assessing risks**

The school takes 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 Powys County Council can accept liability for any material accessed, or any consequences of Internet access. The school's e-safety policy and its implementation will be monitored and reviewed on a regular basis. An Incident Recording Log must be completed if any inappropriate material is viewed.

**Management of School Website and Published Content including Pupil Images**

The School maintains a website which provides a valuable and easily accessible source of information for parents and the community about the School, its policies and management.

Head Teacher is responsible for the management and updating of the website and for ensuring that content is appropriate and in accordance with this Policy. Personal information about staff or pupils will not be published on the website. Contact details will be limited to the School address, telephone number and an email address. Publication of material on the website will respect copyright and E-SAFETY POLICY CAERSWS CP SCHOOL intellectual property rights.

**Management of School Facebook page/website**

The school maintains a Facebook page which celebrates pupils work.

Parents have to sign to say the do not want any images of their child put on the school website/Facebook page (see Digital/Video Images Permission Form.) A copy of each form is kept in the school office and staff are aware to check pupil's in their class for the appropriate consent.

Images which include a pupil's face will be selected carefully even if already published in the media. Associated text will not include the pupil's name or information enabling identification by a stranger. The above rules will be used to educate pupils on the need for caution in publishing personal information and to acknowledge authorship and respect copyright.

**Handling e-safety complaints**

Complaints of internet misuse must be referred to the headteacher. Any complaint about staff misuse must be referred to the headteacher. Complaints of a child protection nature must be dealt with in accordance with the school's child protection policy. Pupils and parents are informed of the complaints procedure. Pupils and parents are informed of the consequences for pupil misuse of the Internet (see Acceptable Use Policy).

**Communications Policy**

**Introducing the e-safety policy to pupils**

Newsletters remind parents and pupils of appropriate use. The Police give e-safety talks annually to Upper Key Stage 2 pupils. Pupils are informed that network and Internet use is monitored and appropriately followed up. The children receive e-safety lessons and are constantly reminded of online safety. In addition every two years NSPCC teach Year 5/6 about Internet safety and dealing with online bullying.

- Useful e–Safety programmes include: Think U Know: www.thinkuknow.co.uk
- Childnet: www.childnet.com
- Kidsmart: www.kidsmart.org.uk
- Safe: www.safesocialnetworking.org

**Staff and the e-safety policy**

All staff receive a copy of the e-safety policy. Staff are informed that network and Internet traffic can be traced to an individual user. The Head receives annual LSCB L3 training updates which cover aspects of Internet safety.

Staff should not use mobile phones in school during teaching hours. Attached in Appendix A are a set of guidelines which take into account the unique position that a teacher has in the school and wider community.

- CEOP (Child Exploitation and Online Protection Centre): www.ceop.police.uk
- Childline: www.childline.org.uk
- Childnet: www.childnet.com

Click Clever Click Safe Campaign: http://clickcleverclicksafe.direct.gov.uk Kidsmart: www.kidsmart.org.uk

- Think U Know website: www.thinkuknow.co.uk

HWB: www.hwb.wales.gov.uk/

- Safer Internet: www.saferinternet.org.uk/

**Enlisting parents' and carers' support**

Parents' and carers' attention is drawn to the school's E-Safety Policy in newsletters the school brochure and on the school prospectus. The school asks all new parents to sign the pupil/parent agreement when they register their child with the school.

**Equality**

In implementing and reviewing this and related policies, the School will avoid unlawful discrimination and will seek to apply the policies consistently to all pupils, parent/carers, staff and visitors irrespective of age, disability, race or ethnic background, gender (sex), gender reassignment, marriage and civil partnership, pregnancy and maternity, religion or belief, or sexual orientation.

**Training, Monitoring, Evaluation and Review**

The Head Teacher is responsible for arranging any necessary or appropriate training of staff on E-Safety and for ensuring that all staff are familiar with this Policy. The E-Safety Coordinator is responsible for monitoring the implementation of this Policy and will evaluate it periodically in consultation with the Head Teacher. The Head Teacher will report any significant developments to the

Governing Body, who will review this Policy annually together with the Child Protection and Safeguarding Policies.

This policy has been agreed by the headteacher, staff, e-safety group and approved by the school governing body.

This policy was written: Jan 2018 and updated in June 2021 using part of the 360 degree Safe Cymru Policy from HWB. The e-safety committee has added a section to this policy. This policy should be read in conjunction with Powys Social Media and E-safety Policy (for staff.)

Date to be reviewed: Annually

Signed: Chair of Governors: C. Rowlands

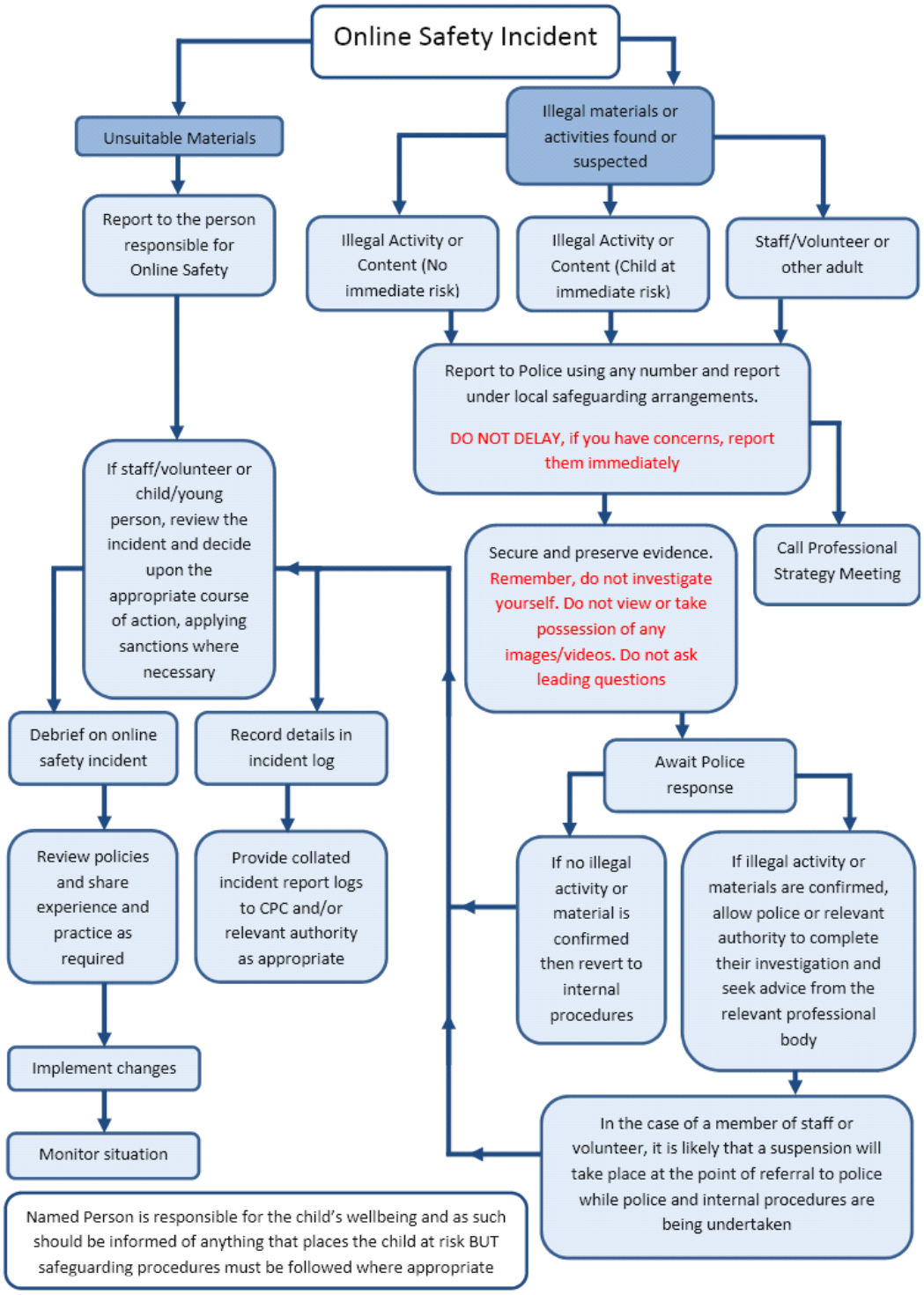
Head Teacher: S M Gabbett

**Appendix A**

Incident Reporting Log

| | | | |
|---|---|---|---|
| **Reporting Log** | **Signature** | | |
| | **Incident Reported by** | | |
| | **Action taken** | **By whom?** | |
| | | **What?** | |
| | **Incident** | | |
| | **Time** | | |
| | **Date** | | |

**Appendix B**


Online Safety Incident
Unsuitable Materials
Illegal materials or activities found or suspected
Report to the person responsible for Online Safety
Illegal Activity or Content (No immediate risk)
Illegal Activity or Content (Child at immediate risk)
Staff/Volunteer or other adult
Report to Police using any number and report under local safeguarding arrangements.
DO NOT DELAY, if you have concerns, report them immediately
If staff/volunteer or child/young person, review the incident and decide upon the appropriate course of action, applying sanctions where necessary
Secure and preserve evidence. Remember, do not investigate yourself. Do not view or take possession of any images/videos. Do not ask leading questions
Call Professional Strategy Meeting
Debrief on online safety incident
Record details in incident log
Await Police response
Review policies and share experience and practice as required
Provide collated incident report logs to CPC and/or relevant authority as appropriate
If no illegal activity or material is confirmed then revert to internal procedures
If illegal activity or materials are confirmed, allow police or relevant authority to complete their investigation and seek advice from the relevant professional body
Implement changes
Monitor situation
In the case of a member of staff or volunteer, it is likely that a suspension will take place at the point of referral to police while police and internal procedures are being undertaken
Named Person is responsible for the child's wellbeing and as such should be informed of anything that places the child at risk BUT safeguarding procedures must be followed where appropriate