# E-SAFETY POLICY

**Background and Rationale**

New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school.

Our school e-safety policy helps to ensure safe and appropriate use of ICT by children at all times.

## Development and Monitoring

This e-safety policy has been developed by the stakeholders involved in the school made up of:

- Headteacher
- Teaching Staff
- Governors
- Parents and Carers
- Members of the School Senedd
- Our Pupil Action Group - Digi Dragons

The school will monitor the impact of the policy using:

- Logs of reported incidents
- Internal monitoring data for network activity
- Surveys / questionnaires of:
    - learners
    - parents / carers
    - staff

## Scope of the Policy

This policy applies to all members of the school community (including staff, pupils, volunteers, parents/carers, visitors, community users) who have access to and are users of school ICT systems, both in and out of school.

The school will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents/carers of incidents of inappropriate e-safety behaviour that take place out of school.

## Roles and Responsibilities

**Headteacher and Senior Leaders:**

- The Headteacher is responsible for ensuring the safety (including e-safety) of members of the school community, though the day to day responsibility for e- safety will be delegated to the ICT/ Tech leader.
- The Headteacher and another member of the Senior Leadership Team 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. (see SWGfL flow chart on dealing with e-safety incidents – included in a later section – "Responding to incidents of misuse" and relevant Local Authority HR / disciplinary procedures).
- *The Headteacher and team are responsible for ensuring that the school's ICT infrastructure is secure and is not open to misuse or malicious attack.*

**Tech Leader/s:**

The Tech Leader/s are responsible for ensuring:

- that the school meets the e-safety technical requirements outlined in the SWGfL Security Policy and Acceptable Usage Policy and any relevant Local Authority E-Safety Policy and guidance.
- that users may only access the school's networks through a properly enforced password protection policy.

**Tech Leader/s and Teaching/Support Staff:**

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 school Acceptable Internet Use Statement.
- they report any suspected misuse or problem to the Headteacher or Tech leader.
- digital communications with pupils (email / Virtual Learning Environment (VLE) / voice) should be on a professional level and only carried out using official school systems.
- e-safety issues are embedded in all aspects of the curriculum and other school activities.
- pupils understand and follow the school e-safety and acceptable use policy.
- pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.
- they monitor ICT activity in lessons, extra curricular and extended school activities.
- they are aware of e-safety issues related to the use of mobile phones, cameras and hand held devices and that they monitor their use and implement current school policies with regard to these devices.

**Learners:**

Learners will be expected to use the ICT systems appropriately and in accordance with teacher guidance and will be expected to sign a child friendly version of the Acceptable Use Policy agreement.

**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. Research shows that many parents and carers do not fully understand

the issues and are less experienced in the use of ICT than their children. The school will therefore take every opportunity to help parents understand these issues through parent learner reviews, open afternoons, newsletters, letters, website and information about e-safety campaigns.

Parents and carers will be responsible for endorsing the Acceptable Use Policy agreement.

**Community Users:**

Community Users who access school ICT systems/ website as part of the Extended School provision will be expected to sign an Acceptable Use Policy agreement before being provided with access to school systems.

## Policy Statements

**Education**

Whilst regulation and technical solutions are very important, their use must be balanced by educating pupils to take a responsible approach. The education of pupils in e-safety is therefore an essential part of the school's e-safety provision. Children and young people need the help and support of the school to recognise and avoid e-safety risks and build their resilience.

E-Safety education will be provided in the following ways:

- A planned e-safety programme should be provided as part of Digital Literacy/PSE/literacy lessons and should be regularly revisited – this will cover both the use of ICT and new technologies in school and outside school.
- Key e-safety messages should be reinforced as part of a planned programme of assemblies.
- Pupils should be taught in all lessons to be critically aware of the material/content they access on-line and be guided to validate the accuracy of information.
- Pupils should be helped to understand the need for the pupil Acceptable Internet Use Statement and encouraged to adopt safe and responsible use of ICT, the internet and mobile devices both within and outside school.
- Staff should act as good role models in their use of ICT, the internet and mobile devices.

## Education – parents / carers

Some parents and carers have only a limited understanding of e-safety risks and issues, yet they play an essential role in the education of their children and in the monitoring / regulation of the children's on-line experiences. Parents often either underestimate or do not realise how often children and young people come across potentially harmful and inappropriate material on the internet and are often unsure about what they would do about it. "There is a generational digital divide". (Byron Report).

The school will therefore seek to provide information and awareness to parents and carers through:

- Letters, newsletters, school website.
- Parent consultations.
- Reference to appropriate websites.

## Education & Training – Staff

It is essential that all staff receive e-safety training and understand their responsibilities, as outlined in this policy.

The school will ensure that all staff are up to date with e-safety procedures. Training will be made available as and when appropriate.

## Technical – infrastructure / equipment, filtering and monitoring

The school will be responsible for ensuring that the school network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also need to ensure that the relevant people named in the above sections will be effective in carrying out their e-safety responsibilities.

School ICT systems will be managed in ways that ensure that the school meets the e- safety technical requirements outlined in the SWGfL Security Policy and Acceptable Usage Policy and any relevant Local Authority E-Safety Policy and guidance.

## Use of digital and video images - Photographic, Video

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 and pupils need to be aware of the risks associated with sharing images and with posting digital images on the internet. Those images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. There are many reported incidents of employers carrying out internet searches for information about potential and existing employees.

The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet eg on social networking sites.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website.
- Learner's work can only be published with the permission of the student / pupil and parents or carers.

***See additional policy on Online Learning & Live Streaming.***

## Data Protection

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 2018 which states that personal data must be:

- Fairly and lawfully processed
- Processed for limited purposes
- Adequate, relevant and not excessive
- Accurate
- Kept no longer than is necessary

- Processed in accordance with the data subject's rights
- Secure
- Only transferred to others with adequate protection.

Staff must ensure that wherever possible they:

- At all times take care to ensure the safekeeping 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.
- When personal data is stored on any portable computer system, USB stick or any other removable media, wherever possible.
- The data must be encrypted and password protected.
- The device must be password protected (many memory sticks / cards and other mobile devices cannot be password protected).
- The device must offer approved virus and malware checking software.
- The data must be securely deleted from the device, in line with school policy once it has been transferred or its use is complete.

**When using communication technologies the school considers the following as good practice:**

- The official school email service may be regarded as safe and secure and is monitored. Staff and pupils should therefore use only the school email service to communicate with pupils and parents**.**
- Users need to be aware that email communications may be monitored.
- Users must immediately report to the nominated person – in accordance with the school policy, the receipt of any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature and must not respond to any such email.
- Any digital communication between staff and pupils or parents/carers must be professional in tone and content.

## Responding to incidents of misuse

It is hoped that all members of the school community will be responsible users of ICT, who understand and follow this policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse.

Listed below are the responses that will be made to any apparent or actual incidents of misuse. If any apparent or actual misuse appears to involve illegal activity e.g:.

- child sexual abuse images
- adult material which potentially breaches the Obscene Publications Act
- criminally racist material
- other criminal conduct, activity or materials

The SWGfL flow chart and http://www.swgfl.org.uk/safety/default.asp should be consulted and actions followed in line with the flow chart, in particular the sections on reporting the incident to the police and the preservation of evidence.

Policy written: November 2015

*Equality and cohesion will be promoted, in line with our Equality and Cohesion Policy, and the policy will be operated in a non-discriminatory way.*

Policy Review Date: February 2017
February 2019
May 2021
November 2023

360 Safe Degree Award achieved November 2019.

Tech Team: Dorian Oldfield, Nicole Cogbill & Rhianna Rose

Safeguarding Governor - Rebecca Lloyd-James

Link Governors - David Powell

**USEFUL ONLINE SAFETY WEBSITES FOR CHILDREN AND PARENTS:**

*Equality and cohesion will be promoted, in line with our Equality and Cohesion Policy, and the policy will be operated in a non-discriminatory way.*

NSPCC - https://www.nspcc.org.uk/preventing-abuse/keeping-children-safe/online-safety/

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

Safety Net Kids - http://www.safetynetkids.org.uk/personal-safety/staying-safe-online/

ThinkuKnow. - https://www.thinkuknow.co.uk/

Kidsmart. - http://www.kidsmart.org.uk/

Childnet - https://www.childnet.com/parents-and-carers/

*Equality and cohesion will be promoted, in line with our Equality and Cohesion Policy, and the policy will be operated in a non-discriminatory way.*