

Ysgol Cynradd Drury

E – Safety Policy

2025 – 2026





# Development / Monitoring / Review of this Policy

This Online Safety policy has been developed by a working group made up of:

- Headteacher
- Online Safety Coordinator
- Staff
- Governors
- Consultation with the whole school community has taken place through a range of formal and informal meetings.

## Schedule for Development / Monitoring / Review:

Policy approved by governors on:

Policy to be reviewed:

The school will monitor the impact of the policy using: *(delete / add as relevant)*

- Logs of reported incidents
- Monitoring logs of internet activity (including sites visited) / filtering
- Internal monitoring data for network activity
- Surveys / questionnaires of
  - students / pupils
  - parents / carers
  - staff

## Scope of the Policy

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

The Education and Inspections Act 2006 empowers Headteachers to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of online-bullying or other Online Safety incidents covered by this policy, which may take place outside of the school, but is linked to membership of the school. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data (see appendix for template policy). In the case of both acts, action can only be taken over issues covered by the published Behaviour Policy.

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 Online Safety behaviour that take place out of school.



## Roles and Responsibilities

The following section outlines the online safety roles and responsibilities of individuals and groups within the school.

### Governors

Governors are responsible for the approval of the Online Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the *Governors* receiving regular information about online safety incidents and monitoring reports. A member of the Governing Body has taken on the role of Online Safety Governor. The role of the Online Safety Governor will include:

- regular meetings with the Online Safety Co-ordinator
- attendance at Online Safety Group meetings
- regular monitoring of online safety incident logs
- regular monitoring of filtering / change control logs
- reporting to relevant Governors

### Headteacher:

- The Headteacher has a duty of care for ensuring the safety (including online safety) of members of the school community, though the day to day responsibility for online safety will be delegated to the Online Safety coordinator
- The Headteacher and (at least) another member of the Senior Leadership Team should be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff. (see flow chart on dealing with online safety incidents – included in a later section – “Responding to incidents of misuse” and relevant Local Authority /disciplinary procedures).

### Online Safety Officer / Lead:

- leads the Online Safety Group
- takes day to day responsibility for online safety issues and has a leading role in establishing and reviewing the school online safety policies / documents
- ensures that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place.
- provides training and advice for staff
- liaises with the Local Authority / MAT / relevant body
- liaises with school technical staff / Governors.
- receives reports of online safety incidents and creates a log of incidents to inform future online safety developments.
- meets regularly with Online Safety Governor / Director to discuss current issues, review incident logs and filtering / change control logs
- attends relevant meeting / committee of Governors / Directors
- reports regularly to Senior Leadership Team



## Local Authority Technical staff:

Local Authority technical support is responsible for ensuring:

- that the school's technical infrastructure is secure and is not open to misuse or malicious attack
- that it meets required online safety technical requirements and any Local Authority Online Safety Policy / Guidance that may apply.
- that users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed
- the filtering policy (if it has one), is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person
- that they keep up to date with online safety technical information in order to effectively carry out their online safety role and to inform and update others as relevant

## Teaching and Support Staff:

Are responsible for ensuring that:

- they have an up to date awareness of online safety matters and of the current school Online Safety Policy and practices
- they have read, understood and signed the Staff Acceptable Use Policy / Agreement (AUP)
- they report any suspected misuse or problem to the Headteacher or Online Safety Officer for investigation / action / sanction.
- all digital communications with pupils / parents / carers should be on a professional level and only carried out using official school systems.

## Designated Safeguarding Lead: Headteacher

Should be trained in Online Safety issues and be aware of the potential for serious child protection / 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
- online-bullying

## Online Safety Group (E-safety Officers):

The Online Safety Group provides a consultative group that has wide representation from the school, with responsibility for issues regarding online safety and the monitoring the Online Safety Policy including the impact of initiatives.

Members of the Online Safety Group (or other relevant group) will assist the Online Safety Officer / Lead (or other relevant person, as above) with:

- the production / review / monitoring of the school Online Safety Policy / documents.

*The more we learn, the more we know,  
Ysgol Drury is a great place to grow.*



- mapping and reviewing the online safety / digital literacy curricular provision – ensuring relevance, breadth and progression
- monitoring network / internet / incident logs
- consulting stakeholders – including parents / carers and the students / pupils about the online safety provision

### **Students / Pupils:**

- are responsible for using the school digital technology systems in accordance with the Pupil Acceptable Use Agreement.
- 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
- will be expected to know and understand policies on the use of mobile devices and digital cameras. They should also know and understand policies on the taking / use of images and on online-bullying.
- should understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the school's / academy's Online 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 / Learning Platform and information about national / local online safety campaigns / literature. Parents and carers will be encouraged to support the school in promoting good online safety practice and to follow guidelines on the appropriate use of:

- digital and video images taken at school events
- access to parents' sections of the website / Learning Platform and on-line student / pupil records
- their children's personal devices in the school.

## **Technical Equipment**

The school will be responsible for ensuring that the school infrastructure / 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 online safety responsibilities.

The LA will also have their own lines of responsibility for ensuring the firewall and security elements are kept up to date and ensure pupils are safe when searching online.



## Mobile Technologies (including BYOD/BYOT)

Mobile technology devices may be school owned/provided or personally owned and might include: smartphone, tablet, notebook / laptop or other technology that usually has the capability of utilising the school's wireless network. The device then has access to the wider internet which may include the school's learning platform and other cloud based services such as email and data storage.

All users should understand that the primary purpose of the use of mobile / personal devices in a school context is educational. The mobile technologies policy should be consistent with and inter-related to other relevant school policies including but not limited to the Safeguarding Policy, Behaviour Policy, Bullying Policy, Acceptable Use Policy, and policies around theft or malicious damage.

The school Acceptable Use Agreements for staff, pupils/students and parents / carers will give consideration to the use of mobile technologies (see appendices)

## 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 pupils need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for cyberbullying to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. It is common for employers to carry 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 e.g. on social networking sites.
- Written permission from parents or carers will be obtained before photographs of students / pupils are published on the school website / social media / local press

See staff / volunteers AUP plus Digital Image permission slips for details.

## Data Protection

With effect from 25th May 2018, the data protection arrangements for the UK change following the European Union General Data Protection Regulation (GDPR) announced in 2016.

Personal data will be recorded, processed, transferred and made available according to the current data protection legislation. The school Privacy Notice and Information Governance Policy gives further details on the collection of this data and how it is shared.



## Communications

A wide range of rapidly developing communications technologies has the potential to enhance learning. The following table shows how the school currently considers the benefit of using these technologies for education outweighs their risks / disadvantages:

Communication Technologies	Staff & other adults		Students / Pupils		
	Allowed	Not allowed	Not allowed	Allowed	Not allowed
Mobile phones may be brought to the school	X				
Use of mobile phones in lessons					
Use of mobile phones in social time					
Taking photos on mobile phones / cameras					
Use of other mobile devices e.g. tablets, gaming devices					
Use of personal email addresses in school, or on school network					
Use of school email for personal emails					
Use of messaging apps					
Use of social media (i.e twitter)					
Use of blogs					

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. Users should be aware that email communications are monitored. Staff and pupils should therefore use only the school email service to communicate with others when in school, or on school network systems.
- Users must immediately report, to the nominated person – in accordance with the school policy, the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.



- Any digital communication between staff and students / pupils or parents / carers (email, social media, chat, blogs, VLE etc) must be professional in tone and content. These communications may only take place on official (monitored) school systems. Personal email addresses, text messaging or social media must not be used for these communications.

## Social Media - Protecting Professional Identity

Please see social Media Policy for full details.

## Dealing with inappropriate material

Some internet activity e.g. accessing child abuse images or distributing racist material is illegal and would obviously be banned from school / academy and all other technical systems. Other activities e.g. cyber-bullying would be banned and could lead to criminal prosecution. There are however a range of activities which may, generally, be legal but would be inappropriate in a school / academy context, either because of the age of the users or the nature of those activities.

The school believes that the activities referred to in the following section would be inappropriate in a context and that users, as defined below, should not engage in these activities in / or outside the school / academy when using school equipment or systems. The school policy restricts usage as follows:

User Actions	Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Users shall not visit internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate					
Child sexual abuse images -The making, production or distribution of indecent images of children. Contrary to The Protection of Children Act 1978					X
Grooming, incitement, arrangement or facilitation of sexual acts against children Contrary to the Sexual Offences Act 2003.					X
Possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character) Contrary to the Criminal Justice and Immigration Act 2008					X
Criminally racist material in UK – to stir up religious hatred (or hatred on the grounds of sexual orientation) – contrary to the Public Order Act 1986					X
Pornography				X	

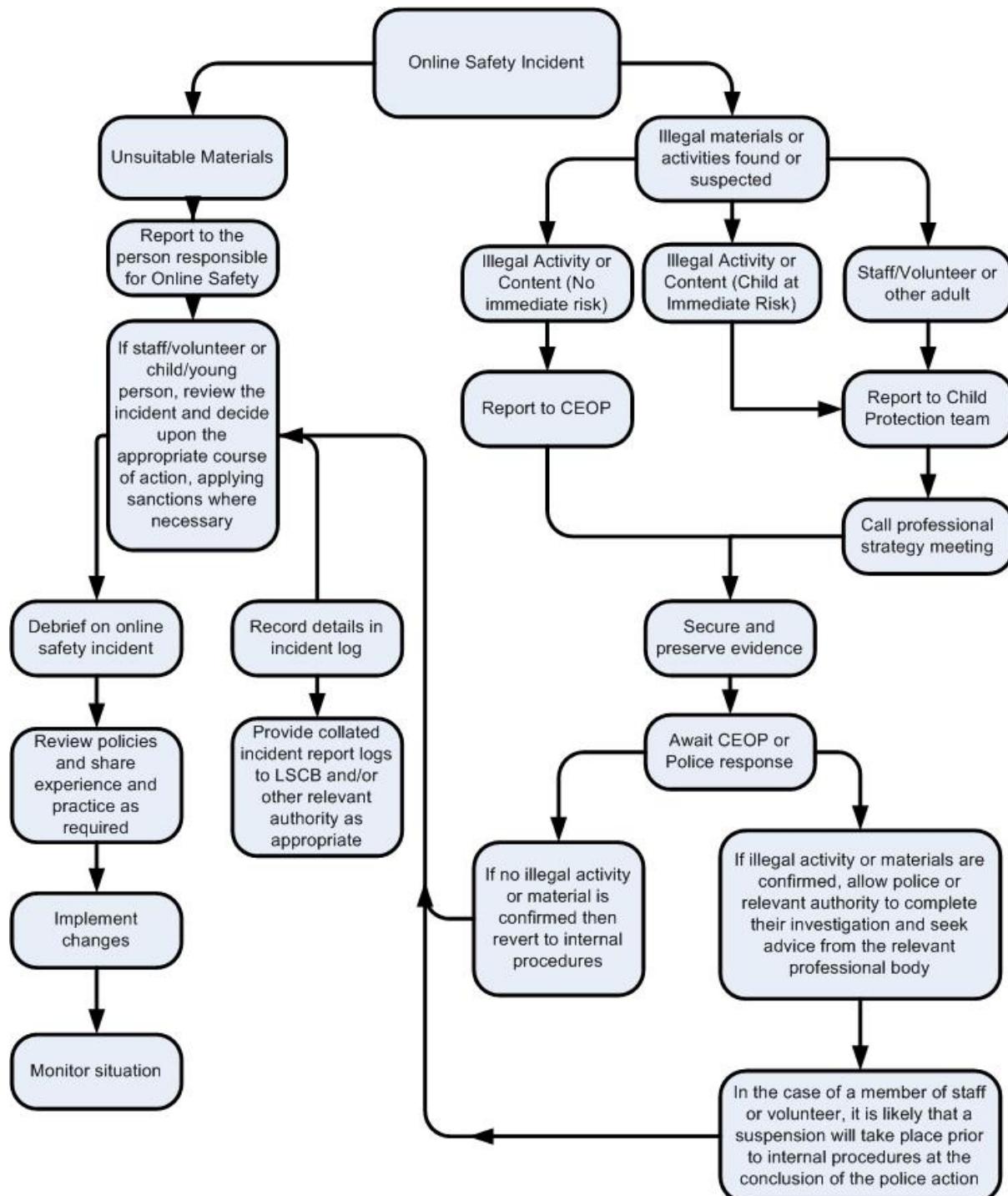


Promotion of any kind of discrimination				X	
threatening behaviour, including promotion of physical violence or mental harm				X	
Promotion of extremism or terrorism				X	
Any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute				X	
Using school systems to run a private business				X	
Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school / academy				X	
Infringing copyright				X	
Revealing or publicising confidential or proprietary information (eg financial / personal information, databases, computer / network access codes and passwords)				X	
Creating or propagating computer viruses or other harmful files				X	
Unfair usage (downloading / uploading large files that hinders others in their use of the internet)				X	
On-line gaming (educational)			X		
On-line gaming (non-educational)				X	
On-line gambling				X	
On-line shopping / commerce				X	
File sharing				X	
Use of social media				X	
Use of messaging apps (other than school email)				X	
Use of video broadcasting e.g. Youtube and uploading own content					X



## Illegal Incidents

If there is any suspicion that the web site(s) concerned may contain child abuse images, or if there is any other suspected illegal activity staff will report these immediately to the Headteacher. Please refer to the Flowchart (below) for responding to online safety incidents and report immediately to the police.





## Other Incidents

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

**In the event of suspicion, all steps in this procedure should be followed:**

- Have more than one senior member of staff involved in this process. This is vital to protect individuals if accusations are subsequently reported.
- Conduct the procedure using a designated computer that will not be used by young people and if necessary can be taken off site by the police should the need arise. Use the same computer for the duration of the procedure.
- It is important to ensure that the relevant staff should have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
- Record the URL of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed and attached to the form (except in the case of images of child sexual abuse – see below)
- Once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does then appropriate action will be required and could include the following:
  - Internal response or discipline procedures
  - Involvement by Local Authority / Academy Group or national / local organisation (as relevant).
  - Police involvement and/or action
- **If content being reviewed includes images of child abuse then the monitoring should be halted and referred to the Police immediately.**  
**Other instances to report to the police would include:**
  - incidents of 'grooming' behaviour
  - the sending of obscene materials to a child
  - adult material which potentially breaches the Obscene Publications Act
  - criminally racist material
  - promotion of terrorism or extremism
  - other criminal conduct, activity or materials
- **Isolate the computer in question as best you can. Any change to its state may hinder a later police investigation.**

It is important that all of the above steps are taken as they will provide an evidence trail for the school / academy and possibly the police and demonstrate that visits to these sites were carried out for safeguarding purposes. The completed form should be retained by the group for evidence and reference purposes.

## School Actions & Sanctions

It is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the school community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal behaviour / disciplinary procedures as follows:



Pupils Incidents	Refer to Headteacher	Refer to Police	Refer to technical support staff for action re filtering / concerns, etc.	Inform parents / carers	Removal of network / internet access rights	Warning	Further sanction ea detention / exclusion
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).	X X		X X				
Unauthorised use of non-educational sites during lessons					X		
Unauthorised / inappropriate use of mobile phone / digital camera / other mobile device	X						
Unauthorised / inappropriate use of social media / messaging apps / personal email	X						
Unauthorised downloading or uploading of files				X		X	
Allowing others to access school network by sharing username and passwords	X			X X X			
Attempting to access or accessing the school network, using another student's / pupil's account					X		
Attempting to access or accessing the school / academy network, using the account of a member of staff	X		X		X		
Corrupting or destroying the data of other users					X		



Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature	X		X		X	
Continued infringements of the above, following previous warnings or sanctions					X	
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school	X	X	X	X	X	X
Using proxy sites or other means to subvert the school's filtering system	X	X	X	X	X	
Accidentally accessing offensive or pornographic material and failing to report the incident			X		X	
Deliberately accessing or trying to access offensive or pornographic material	X	X				
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act	X	X	X	X		



## Staff Incidents

	Refer to line manager	Refer to Headteacher / Principal	Refer to Local Authority / HR	Refer to Police	Refer to Technical Support Staff for action re filtering etc.	Warning	Suspension	Disciplinary action
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).	X	X	X					
Inappropriate personal use of the internet / social media / personal email	X							
Unauthorised downloading or uploading of files	X					X		
Allowing others to access school network by sharing username and passwords or attempting to access or accessing the school network, using another person's account	X	X				X		
Careless use of personal data e.g. holding or transferring data in an insecure manner	X						X	
Deliberate actions to breach data protection or network security rules	X		X				X	
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software		X	X					X
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature	X					X	X	
Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with students / pupils	X							X
Actions which could compromise the staff member's professional standing	X						X	X
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school / academy	X						X	X
Using proxy sites or other means to subvert the school's filtering system	X	X	X					X
Accidentally accessing offensive or pornographic material and failing to report the incident	X					X		
Deliberately accessing or trying to access offensive or pornographic material	X		X					X
Breaching copyright or licensing regulations	X							
Continued infringements of the above, following previous warnings or sanctions	X							X



## Appendix

SWGfL Online Safety Policy Templates

Staff AUP

Pupil and parent AUP