



**HAPUSRWYDD ▪ HYDER ▪ LLWYDDIANT**  
**HAPPINESS ▪ CONFIDENCE ▪ SUCCESS**



## **Ffederasiwn Dyffryn Ceiriog Ceiriog Valley Federation**

### **Online Safety Policy**

---

Approved by Governing Body on	Date: July 2021
Due for review on	Date: July 2024
Signed by Chair of Governing Body	
(Print name)	Emyr Owens

## Development / Monitoring / Review of this Policy

This e-Safety policy has been developed by a working group / committee made up of:

- Headteacher
- E-Safety Coordinator
- Staff – including Teachers
- Governors
- Parents and Carers
- Community users

Consultation with the whole school community has taken place through a range of formal and informal meetings.

### Schedule for Development / Monitoring / Review

This e-Safety policy was approved by the Governing Body / Governors Sub Committee on:	July 2021
The implementation of this e-Safety policy will be monitored by the:	Child Protection Officer, e-Safety Coordinator, Senior Leadership Team, Governors.
Monitoring will take place at regular intervals:	At least once a year
The Governing Body / Governors Sub Committee will receive a report on the implementation of the e-Safety policy generated by the monitoring group (which will include anonymous details of e-Safety incidents) at regular intervals:	At least once a year
The e-Safety Policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to e-Safety or incidents that have taken place. The next anticipated review date will be:	September 2024
Should serious e-Safety incidents take place, the following Internal/external persons / agencies should be informed:	Mrs L. Sockett, Miss B. Evans, Mrs Harper (Governor) John Hodgson (LA Safeguarding Officer), Police

The school will monitor the impact of the policy using:

- Logs of reported incidents
  - Monitoring logs of internet activity (including sites visited)
  - Internal monitoring data for network activity
  - Surveys / questionnaires of
    - students / pupils
    - parents / carers
    - staff
- } Will require the assistance of service provider (Council)

## 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 Governing body / Governor's sub-committee receiving regular information about e-Safety incidents and monitoring reports. A member of the Governing Body should take on the role of e-Safety Governor to include:

- regular meetings with the e-Safety Co-ordinator / Officer
- regular monitoring of e-Safety incident logs
- regular monitoring of filtering / change control logs (where possible)
- reporting to relevant Governors / sub-committee / meeting

### **Headteacher / Principal and Senior Leaders:**

- The Headteacher has a duty of care for ensuring the safety (including e-Safety) of members of the school community, though the day to day responsibility for e-Safety may be delegated to the e-Safety Co-ordinator / Officer.
- 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 e-Safety allegation being made against a member of staff.
- The Headteacher / Senior Leaders are responsible for ensuring that the e-Safety Coordinator / Officer and other relevant staff receive suitable training to enable them to carry out their e-Safety roles and to train other colleagues, as relevant.
- The Headteacher / Senior Leaders will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal e-Safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.
- The Senior Leadership Team / Senior Management Team will receive regular monitoring reports from the e-Safety Co-ordinator / Officer.

### **E-Safety Coordinator / Officer:**

E-safety responsibility in  
Ysgol Llanarmon Dyffryn Ceiriog-Sian Roscoe  
Ysgol Cynddelw –Beth Evans

Overall responsibility lies with the ICT coordinator Miss Beth Evans.

### **The E-Safety Coordinator / Officer**

- leads the e-Safety committee
- 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 / relevant body
- 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 meeting / sub-committee of Governors
- reports regularly to Senior Leadership Team

## **Network Manager (LA):**

The Network Manager (LA) is responsible for ensuring:

- that the school's technical infrastructure is secure and is not open to misuse or malicious attack
- that the school meets (as a minimum) the required e-Safety technical requirements as identified by the Local Authority or other relevant body and also the e-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
- that the filtering policy, is applied and updated on a regular basis and its implementation is not the sole responsibility of any single person.
- that they keep up to date with e-Safety technical information in order to effectively carry out their e-Safety role and to inform and update others as relevant
- that the use of the network / internet / Virtual Learning Environment / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the Headteacher / Senior Leader; e-Safety Coordinator / Officer for investigation / action / sanction

## **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 / Agreement (AUP / AUA)
- they report any suspected misuse or problem to the Headteacher / Senior Leader ; e-Safety Coordinator for investigation / action
- all digital communications with pupils / parents / carers 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 activities
- students / pupils understand and follow the e-Safety and acceptable use agreements / policies
- pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- they monitor the use of digital technologies, mobile devices, cameras etc in lessons and other school activities (where allowed) and implement current policies with regard to these devices
- in lessons where internet use is pre-planned pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches

## **Safeguarding Designated Person**

**NOTE: It is important to emphasise that these are safeguarding issues, not technical issues; the technology provides additional means for safeguarding issues to develop. Some schools may choose to combine the role of Safeguarding Officer and e-Safety Officer.**

The Safeguarding Designated Person should be trained in e-Safety issues and be 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. Depending on the size or structure of the school this committee may be part of the safeguarding group. The group will also be responsible for regular reporting to the Governing Body.

Members of the e-Safety Group will assist the e-Safety Coordinator / Officer with:

- the production / review / monitoring of the school e-Safety policy / documents.
- the production / review / monitoring of the school filtering policy and requests for filtering changes.
- mapping and reviewing the e-Safety curricular provision – ensuring relevance, breadth and progression
- monitoring network / internet / incident logs where possible
- consulting stakeholders – including parents / carers and the students / pupils about the e-Safety provision
- monitoring improvement actions identified through use of the 360 degree safe Cymru self review tool

An e-Safety Group Terms of Reference Template can be found in the appendices (B4)

### **Students / pupils:**

- are responsible for using the school digital technology systems in accordance with the Pupil Acceptable Use Agreement (A1)
- 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 cyber-bullying.
- 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 / VLE and information about national / local e-Safety campaigns / literature. Parents and carers will be encouraged to support the school in promoting good e-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 / VLE
- their children's personal devices in the school (where this is allowed)

### **Community Users**

Community Users who access school systems / website / VLE as part of the wider school provision will be expected to sign a Community User AUA before being provided with access to school systems. (A6)

# Policy Statements

## Education – young people

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 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: (Note: statements will need to be adapted, depending on school structure and the age of the students / pupils)

- A planned e-Safety curriculum should be provided as part of ICT / Computing / PSE / Digital Literacy lessons or other lessons and should be regularly revisited
- Key e-Safety messages should be reinforced as part of a planned programme of assemblies and tutorial / pastoral activities
- Pupils should be taught in 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
- Pupils should be helped to understand the need for the pupil Acceptable Use Agreement and encouraged to adopt safe and responsible use both within and outside school
- Staff should act as good role models in their use of digital technologies the internet and mobile devices
- in lessons where internet use is pre-planned, it is best practice that pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.
- Where pupils are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit.

## Education – parents / carers

Many 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 behaviour. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.

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

- Curriculum activities
- Extra Curricular activities – after school club
- Letters, newsletters, web site, VLE, social media
- Parents / Carers evenings / sessions
- High profile events / campaigns eg Safer Internet Day
- Reference to the relevant web sites / publications eg <https://hwb.wales.gov.uk/>  
[www.saferinternet.org.uk/](http://www.saferinternet.org.uk/) <http://www.childnet.com/parents-and-carers>  
(see appendix for further links / resources)

## Education – The Wider Community

The school will provide opportunities for local community groups / members of the community to gain from the school's e-Safety knowledge and experience. This may be offered through the following:

- e-Safety messages targeted towards grandparents and other relatives as well as parents.
- The school VLE / website will provide e-Safety information for the wider community
- Supporting community groups eg Early Years Settings, Childminders, youth / sports / voluntary groups to enhance their e-Safety provision (possibly supporting the group in the use of Online Compass, an online safety self review tool - [www.onlinecompass.org.uk](http://www.onlinecompass.org.uk))

## **Education & Training – Staff / Volunteers**

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. An audit of the e-Safety training needs of all staff will be carried out regularly. It is expected that some staff will identify e-Safety as a training need within the performance management process.
- 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 Agreements.
- The e-Safety Coordinator / Officer (or other nominated person) will receive regular updates through attendance at external training events (eg from Consortium / SWGfL / LA / other relevant organisations) and by reviewing guidance documents released by relevant organisations.
- This e-Safety policy and its updates will be presented to and discussed by staff in staff / team meetings / INSET days.
- The e-Safety Coordinator / Officer (or other nominated person) will provide advice / guidance / training to individuals as required.

## **Training – Governors**

Governors should take part in e-Safety training / awareness sessions, with particular importance for those who are members of any sub committee / group involved in technology / e-Safety / health and safety / safeguarding . This may be offered in a number of ways:

- Attendance at training provided by the Local Authority / National Governors Association / or other relevant organisation (eg SWGfL).
- Participation in school training / information sessions for staff or parents.

## **Technical – infrastructure / equipment, filtering and monitoring**

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 e-Safety responsibilities:

- School technical systems will be managed in ways that ensure that the school meets recommended technical requirements
- There will be regular reviews and audits of the safety and security of school technical systems
- Servers, wireless systems and cabling must be securely located and physical access restricted
- All users will have clearly defined access rights to school technical systems and devices.
- All users will be provided with a username and secure password by the class teacher who will keep an up to date record of users and their usernames. Users are responsible for the security of their username and password
- LA and school is responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations (Inadequate licencing could cause the school to breach the Copyright Act which could result in fines or unexpected licensing costs)
- Internet access is filtered for all users. Illegal content (child sexual abuse images) is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list. Content lists are regularly updated and internet use is logged and regularly monitored. There is a clear process in place to deal with requests for filtering changes (see appendix for more details)
- Where possible, school technical staff regularly monitor and record the activity of users on the school technical systems and users are made aware of this in the Acceptable Use Agreement.
- An appropriate system is in place for users to report any actual / potential technical incident / security breach to the relevant person, as agreed).
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, mobile devices etc from accidental or malicious attempts which might threaten the security of the school systems and data. These are tested regularly. The school infrastructure and individual workstations are protected by up to date virus software.

- An agreed policy is in place for the provision of temporary access of “guests” (eg trainee teachers, supply teachers, visitors) onto the school systems.
- An agreed policy is in place regarding the extent of personal use that users (staff / students / pupils / community users) and their family members are allowed on school devices that may be used out of school.
- An agreed policy is in place regarding the use of removable media (eg memory sticks / CDs / DVDs) by users on school devices. Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured. (see School Personal Data Policy Template in the appendix for further detail)

## 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. 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 eg on social networking sites.
- In accordance with guidance from the Information Commissioner's Office, parents / carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use is not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published / made publicly available on social networking sites, nor should parents / carers comment on any activities involving other pupils in the digital / video images.
- Staff and volunteers are allowed to take digital / video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment, the personal equipment of staff should not be used for such purposes.
- Care should be taken when taking digital / video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with good practice guidance on the use of such images.
- Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website.
- Pupil's work can only be published with the permission of the pupil and parents or carers.

## Data Protection

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

The school must ensure 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”. (see Privacy Notice section in the appendix)
- It has a Data Protection Policy (see appendix for template policy)
- It is registered as a Data Controller for the purposes of the Data Protection Act (DPA)
- Responsible persons are appointed / identified - Senior Information Risk Officer (SIRO) and Information Asset Owners (IAOs)
- Risk assessments are carried out
- It has clear and understood arrangements for the security, storage and transfer of personal data
- Data subjects have rights of access and there are clear procedures for this to be obtained
- There are clear and understood policies and routines for the deletion and disposal of data
- There is a policy for reporting, logging, managing and recovering from information risk incidents
- There are clear Data Protection clauses in all contracts where personal data may be passed to third parties
- There are clear policies about the use of cloud storage / cloud computing which ensure that such data storage meets the requirements laid down by the Information Commissioner’s Office.

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.

When personal data is stored on any portable computer system, memory stick or any other removable media:

- 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 (below) once it has been transferred or its use is complete

The Personal Data Handling Policy in appendix B2 provides more detailed guidance on the school’s responsibilities and on good practice.

## Communications

This is an area of rapidly developing technologies and uses. Schools will need to discuss and agree how they intend to implement and use these technologies eg few schools allow pupils to use mobile phones in lessons, while others identify educational potential and allow their use. This section may also be influenced by the age of the pupils. The table has been left blank for school to choose its own responses.

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:

	Staff & other adults			Pupils				
	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission	Not allowed
<b>Communication Technologies</b>								
Mobile phones may be brought to school	✓						✓	
Use of mobile phones in lessons		✓					✓	
Use of mobile phones in social time	✓			✓				
Taking photos on mobile phones / cameras (not on personal phones)	✓				✓			
Use of other mobile devices eg 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		✓					✓	
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 systems (eg by remote access).
- 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 pupils or parents / carers (email, chat, 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.
- Pupils should be taught about e-Safety issues, such as the risks attached to the sharing of personal details. They should also be taught strategies to deal with inappropriate communications and be reminded of the need to communicate appropriately when using digital technologies.
- Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff.

## Social Media - Protecting Professional Identity

With an increase in use of all types of social media for professional and personal purposes a policy that sets out clear guidance for staff to manage risk and behaviour online is essential. Core messages should include the protection of pupils, the school and the individual when publishing any material online. Expectations for teachers' professional conduct are set out by the General Teaching Council Wales (GTCW) but all adults working with children and young people must understand that the nature and responsibilities of their work place them in a position of trust and that their conduct should reflect this.

All schools and local authorities have a duty of care to provide a safe learning environment for pupils and staff. Schools and local authorities could be held responsible, indirectly for acts of their employees in the course of their employment. Staff members who harass, cyberbully, discriminate on the grounds of sex, race or disability or who defame a third party may render the school or local authority liable to the injured party. Reasonable steps to prevent predictable harm must be in place. All staff working at any educational establishment are expected to demonstrate a professional approach and respect for pupils and their families and for colleagues and the learning setting.

The school provides the following measures to ensure reasonable steps are in place to minimise risk of harm to pupils, staff and the school through limiting access to personal information:

- Training to include: acceptable use; social media risks; checking of settings; data protection; reporting issues.
- Clear reporting guidance, including responsibilities, procedures and sanctions
- Risk assessment, including legal risk

School staff should ensure that:

- No reference should be made in social media to pupils, parents / carers or school staff
- They do not engage in online discussion on personal matters relating to members of the school community
- Personal opinions should not be attributed to the school or local authority
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

The school's use of social media for professional purposes will be checked regularly by the senior risk officer and e-Safety committee to ensure compliance with the Social Media, Data Protection, Communications, Digital Image and Video Policies.

## Unsuitable / inappropriate activities

Some internet activity eg accessing child abuse images or distributing racist material is illegal and would obviously be banned from school and all other technical systems. Other activities eg 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 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 school context and that users, as defined below, should not engage in these activities in school or outside school 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
------------	-----------------------------	--------------------------------	--------------	--------------------------

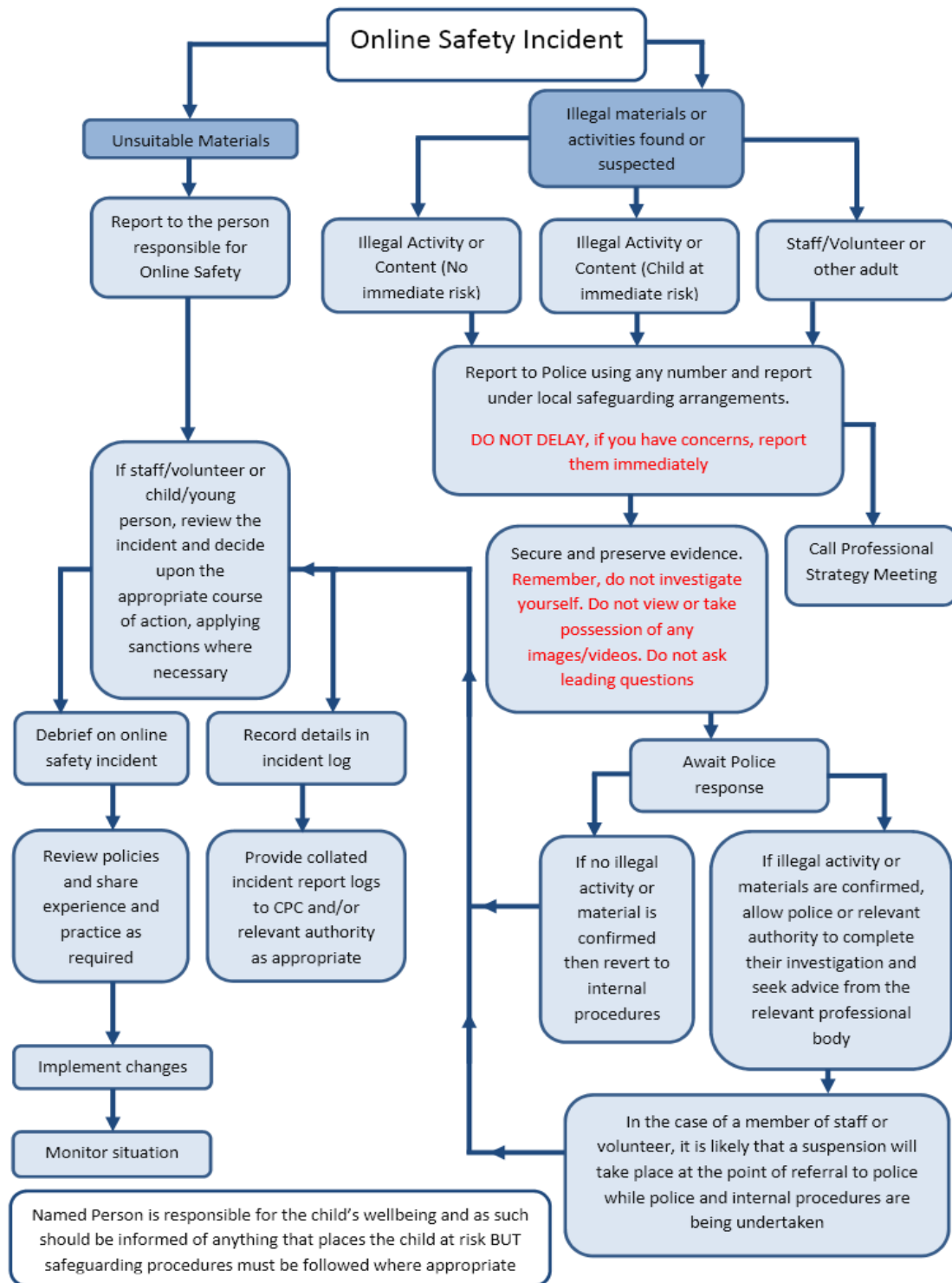
Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	Child sexual abuse images –The making, production or distribution of indecent images of children. Contrary to The Protection of 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	
	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				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)		✓				
On-line gaming (non educational)		✓				
On-line gambling				✓		
On-line shopping / commerce		✓				
File sharing		✓				
Use of social media		✓				
Use of messaging apps		✓				
Use of video broadcasting eg Youtube		✓				

## Responding to incidents of misuse

This guidance is intended for use when staff need to manage incidents that involve the use of online services. It encourages a safe and secure approach to the management of the incident. Incidents might involve illegal or inappropriate activities (see “User Actions” above).

### 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, refer to the right hand side of the Flowchart (below and appendix) 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 / volunteer 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 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
    - 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 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**

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:

**Students / Pupils**

**Actions**

---

Incidents:	Refer to class teacher	Refer to Esafety co-ordinator	Refer to Headteacher / Principal	Refer to Police	Refer to technical support staff for action re filtering / security etc	Inform parents / carers	Removal of network / internet access rights	Warning	Further sanction eg detention / exclusion
<b>Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).</b>		X	X	X	✓				
Unauthorised use of non-educational sites during lessons	✓								
Unauthorised use of mobile phone / digital camera / other mobile device	✓								
Unauthorised use of social media / messaging apps / personal email	✓								
Unauthorised downloading or uploading of files		✓							
Allowing others to access school network by sharing username and passwords	✓	✓	✓						
Attempting to access or accessing the school network, using another student's / pupil's account	✓	✓	✓						
Attempting to access or accessing the school network, using the account of a member of staff	✓	✓	✓						
Corrupting or destroying the data of other users	✓	✓	✓						
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature	✓	✓	✓						
Continued infringements of the above, following previous warnings or sanctions	✓	✓	✓			✓	✓	✓	
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school	✓	✓	✓			✓	✓	✓	
Using proxy sites or other means to subvert the school's filtering system	✓	✓	✓		✓	✓	✓	✓	✓
Accidentally accessing offensive or pornographic material and failing to report the incident	✓	✓	✓						
Deliberately accessing or trying to access offensive or pornographic material	✓	✓	✓			✓	✓	✓	✓
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act	✓	✓	✓		✓				

**Staff**

**Actions**

Incidents:	Refer to line safety co-ordinator	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
<b>Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).</b>		X	X	X	✓	✓	✓	✓
Inappropriate personal use of the internet / social media / personal email	✓	✓	✓		✓	✓		✓
Unauthorised downloading or uploading of files	✓	✓	✓		✓	✓		✓
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	✓	✓	✓		✓	✓		✓
Careless use of personal data eg holding or transferring data in an insecure manner	✓	✓	✓			✓		
Deliberate actions to breach data protection or network security rules	✓	✓	✓	✓	✓	✓	✓	✓
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software	✓	✓	✓	✓	✓	✓	✓	✓
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature	✓	✓	✓	✓	✓	✓	✓	✓
Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with students / pupils	✓	✓	✓	✓	✓	✓	✓	✓
Actions which could compromise the staff member's professional standing	✓	✓	✓	✓	✓	✓	✓	✓
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school	✓	✓	✓	✓	✓	✓	✓	✓
Using proxy sites or other means to subvert the school's filtering system	✓	✓	✓	✓	✓	✓	✓	✓
Accidentally accessing offensive or pornographic material and failing to report the incident	✓	✓	✓		✓	✓		
Deliberately accessing or trying to access offensive or pornographic material	✓	✓	✓	✓	✓	✓	✓	✓
Breaching copyright or licensing regulations	✓	✓	✓	✓	✓	✓	✓	✓
Continued infringements of the above, following previous warnings or sanctions	✓	✓	✓	✓	✓	✓	✓	✓



# Appendix

## Appendices – Section A - Acceptable Use Agreement

- A1 Pupil Acceptable Use Agreement 19
- A2 Staff and Volunteers Acceptable Use Agreement 20
- A3 Parents / Carers Acceptable Use Agreement 23

## Appendices – Section B – Specific Policies

- B1 School Technical Security Policy 28
- B2 School Personal Data Policy 34
- B3 School e-Safety Committee Terms of Reference 47

## Appendices – Section C – Support documents and links

- C1 Responding to incidents of misuse – flowchart 49
- C2 Record of reviewing sites (for internet misuse) 50
- C3 School Reporting Log 52
- C4 School Training Needs Audit 53
- C5 Summary of Legislation 54
- C6 Office 365 – further details 57
- C8 Glossary of terms 59



HAPUSRWYDD • HYDER • LLWYDDIANT  
HAPPINESS • CONFIDENCE • SUCCESS



## Learner Acceptable Use Agreement

### Foundation Phase

- I will ask a teacher or other adult before I use a computer.
- I will only use activities that a teacher or another adult has told me to use.
- I will take care of the computer and other equipment.
- I will ask for help if I am not sure what to do.
- I will be polite and won't get upset or be unkind to anyone.
- I will tell an adult if I see something that upsets me on the screen.
- I will be safe. I won't tell anyone where I live or give them my phone number.
- I know if I break the rules I may not be able to use the computer.



### KS2

For my own personal safety:

- I understand that the school will monitor my use of systems, devices and digital communications
- I will keep my username and password safe and secure – I will not share it, nor will I try to use any other person's username and password.
- I will be aware of "stranger danger", when I am communicating online and won't share personal information about myself or others when online.

I understand that everyone has equal rights to use technology and:

- I understand that the school systems and devices are only to be used for educational reasons and that I will only use them for fun or personal use if I have permission

I will act as I expect others to act toward me:

- I will respect others' work and property and will only copy, remove or alter any other user's files, with the owner's (and teacher's) knowledge and permission
- I will be polite and responsible when I communicate with others,
- I will only take or distribute images of others with their permission.

I understand that the school has to make sure the technology I use is safe and secure so:

- I will not try to use any programmes or software that might allow me to bypass the filtering/security systems in place to prevent access to such materials
- I will immediately report any damage or faults involving equipment or software, however this may have happened

When using the internet for research or fun, I understand that:

- I should make sure that I have permission to use the original work of others in my own work
- Where work is protected by copyright, I will not try to download copies (including images, music and videos)

I understand that I am responsible for my actions, both in and out of school:

- I understand that the school also has the right to take action against me if I am involved in incidents of inappropriate behaviour, that are covered in this agreement, when I am out of school and where they involve my membership of the school community (examples would be cyber-bullying, use of images or personal information)
- I understand that if I don't follow the rules in this acceptable use agreement, there will be consequences. This may include not being allowed to use school technologies.

A2

Staff

# Acceptable Use Policy Agreement



HAPUSRWYDD • HYDER • LLWYDDIANT  
HAPPINESS • CONFIDENCE • SUCCESS



## School Policy

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. The internet and other digital information and communications technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. They also bring opportunities for staff to be more creative and productive in their work. All users should have an entitlement to safe internet access at all times.

### This Acceptable Use Policy is intended to ensure:

- that staff and volunteers will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- that school ICT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that staff are protected from potential risk in their use of ICT in their everyday work.

The school will try to ensure that staff and volunteers will have good access to ICT to enhance their work, to enhance learning opportunities for *students / pupils* learning and will, in return, expect staff and volunteers to agree to be responsible users.

## Acceptable Use Policy Agreement

I understand that I must use school ICT systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the ICT systems and other users. I recognise the value of the use of ICT for enhancing learning and will ensure that students / pupils receive opportunities to gain from the use of ICT. I will, where possible, educate the young people in my care in the safe use of ICT and embed e-Safety in my work with young people.

### For my professional and personal safety:

- I understand that the school will monitor my use of the ICT systems, email and other digital communications.
- I understand that the rules set out in this agreement also apply to use of school ICT systems (eg laptops, email, VLE etc) out of school, and to the transfer of personal data (digital or paper based) out of school.
- I understand that the school ICT systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within the policies and rules set down by the school. (schools should amend this section in the light of their policies which relate to the personal use, by staff and volunteers, of school systems)
- I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may steal it.
- I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person.

### I will be professional in my communications and actions when using school ICT systems:

- I will not access, copy, remove or otherwise alter any other user's files, without their express permission.
- I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will ensure that when I take and / or publish images of others I will do so with their permission and in accordance with the school's policy on the use of digital / video images. I will not use my personal equipment to record these images, unless I have permission to do so. Where these images are published (eg on the school website / VLE) it will not be possible to identify by name, or other personal information, those who are featured.
- I will only use chat and social networking sites in school in accordance with the school's policies. (schools should amend this section to take account of their policy on access to social networking and similar sites)
- I will only communicate with students / pupils and parents / carers using official school systems. Any such communication will be professional in tone and manner. (schools should amend this section to take account of their policy on communications with students / pupils and parents / carers. Staff should be made aware of the risks attached to using their personal email addresses / mobile phones / social networking sites for such communications)
- I will not engage in any on-line activity that may compromise my professional responsibilities.

### **The school and the local authority have the responsibility to provide safe and secure access to technologies and ensure the smooth running of the school :**

- When I use my mobile devices (PDAs / laptops / mobile phones / USB devices etc) in school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment. I will also follow any additional rules set by the school about such use. I will ensure that any such devices are protected by up to date anti-virus software and are free from viruses.
- I will not open any hyperlinks in emails or any attachments to emails, unless the source is known and trusted , or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes)
- I will ensure that my data is regularly backed up, in accordance with relevant school policies.
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings, unless this is allowed in school policies. (schools / academies should amend this section in the light of their policies on installing programmes / altering settings)
- I will not disable or cause any damage to school equipment, or the equipment belonging to others.
- I will only transport, hold, disclose or share personal information about myself or others, as outlined in the School / LA Personal Data Policy (or other relevant policy). Where digital personal data is transferred outside the secure local network, it must be encrypted. Paper based Protected and Restricted data must be held in lockable storage.
- I understand that data protection policy requires that any staff or student / pupil data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by school policy to disclose such information to an appropriate authority.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.

### **When using the internet in my professional capacity or for school sanctioned personal use:**

- I will ensure that I have permission to use the original work of others in my own work
- Where work is protected by copyright, I will not download or distribute copies (including music and videos).

### **I understand that I am responsible for my actions in and out of the school:**

- I understand that this Acceptable Use Agreement applies not only to my work and use of school ICT equipment in school, but also applies to my use of school ICT systems and equipment off the premises and my use of personal equipment on the premises or in situations related to my employment by the school.
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I could be subject to disciplinary action. This could include (schools should amend this section to provide relevant sanctions as per their behaviour policies) a warning, a suspension, referral to Governors and / or the Local Authority and in the event of illegal activities the involvement of the police.

I have read and understand the above and agree to use the school ICT systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) within these guidelines.

Staff / Volunteer Name

Signed

Date



## Ceiriog Valley Federation Parent/Carer Acceptable Use Agreement

### School Policy

Digital technologies have become integral to the lives of children and young people, both within schools and outside school. These technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. Young people should have an entitlement to safe internet access at all times.

### This Acceptable Use Agreement is intended to ensure:

- that young people will be responsible users and stay safe while using the internet and other digital technologies for educational, personal and recreational use.
- that school systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.

The school will try to ensure that *students / pupils* will have good access to digital technologies to enhance their learning and will, in return, expect the *students / pupils* to agree to be responsible users.

### Acceptable Use Agreement

I understand that I must use school ICT systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the ICT systems and other users.

#### For my own personal safety:

- I understand that the school will monitor my use of IT systems, devices and digital communications.
- I will keep my username and password safe and secure – I will not share it, nor will I try to use any other person’s username and password. I understand that I should not write down or store a password where it is possible that someone may steal it.
- I will be aware of “stranger danger”, when I am communicating on-line.
- I will not disclose or share personal information about myself or others when on-line (this could include names, addresses, email addresses, telephone numbers, age, gender, educational details, financial details etc )
- If I arrange to meet people off-line that I have communicated with on-line, I will do so in a public place and take an adult with me.
- I will immediately report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it on-line.

#### I understand that everyone has equal rights to use technology as a resource and:

- I understand that the school systems and devices are primarily intended for educational use and that I will not use them for personal or recreational use unless I have permission.
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not use the school systems or devices for on-line gaming, on-line gambling, internet shopping, file sharing, or video broadcasting (eg YouTube), unless I have permission of a member of staff to do so.
- 

#### I will act as I expect others to act toward me:

- I will respect others’ work and property and will not access, copy, remove or otherwise alter any other user’s files, without the owner’s knowledge and permission.
- I will be polite and responsible when I communicate with others, I will not use strong, aggressive or inappropriate language and I appreciate that others may have different opinions.

- I will not take or distribute images of anyone without their permission.

**I recognise that the school has a responsibility to maintain the security and integrity of the technology it offers me and to ensure the smooth running of the school:**

- I will only use my own personal device(s) in school if I have
- I understand that, if I do use my own device(s) in the school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment.
- I understand the risks and will not try to upload, download or access any materials which are illegal or inappropriate or may cause harm or distress to others, nor will I try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.
- I will not open any hyperlinks in emails or any attachments to emails, unless I know and trust the person / organisation who sent the email, or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes)
- I will not install or attempt to install or store programmes of any type on any school device, nor will I try to alter computer settings.
- I will only use social media sites with permission and at the times that are allowed
- 

**When using the internet for research or recreation, I recognise that:**

- I should ensure that I have permission to use the original work of others in my own work
- Where work is protected by copyright, I will not try to download copies (including music and videos)
- When I am using the internet to find information, I should take care to check that the information that I access is accurate, as I understand that the work of others may not be truthful and may be a deliberate attempt to mislead me.

**I understand that I am responsible for my actions, both in and out of school:**

- I understand that the school also has the right to take action against me if I am involved in incidents of inappropriate behaviour, that are covered in this agreement, when I am out of school and where they involve my membership of the school community (examples would be cyber-bullying, use of images or personal information).
- I understand that if I fail to comply with this Acceptable Use Agreement, I will be subject to disciplinary action. This may include loss of access to the school network / internet, detentions, suspensions, contact with parents and in the event of illegal activities involvement of the police.

**Please complete the sections on the next page to show that you have read, understood and agree to the rules included in the Acceptable Use Agreement. If you do not sign and return this agreement, access will not be granted to school systems and devices.**

### **Pupil Acceptable Use Policy Agreement**

This form relates to the *student / pupil* Acceptable Use Agreement, above.

**This is how we stay safe when we use computers:**

I will ask a teacher or another adult from the school if I want to use the computers

I will only use activities that a teacher or another adult from the school has told or allowed me to use.

I will take care of the computer and other equipment

I will ask for help from a teacher or another adult from the school if I am not sure what to do or if I think I have done something wrong.

I will tell a teacher or another adult from the school if I see something that upsets me on the screen.

I know that if I break the rules I might not be allowed to use a computer.

B1



HAPUSRWYDD ▪ HYDER ▪ LLWYDDIANT  
HAPPINESS ▪ CONFIDENCE ▪ SUCCESS



## Ffederasiwn Dyffryn Ceiriog Ceiriog Valley Federation

### School Technical Security Policy (including filtering and passwords)

---

Approved by Governing Body on	Date:
Due for review on	Date: May 2022
Signed by Chair of Governing Body	
(Print name)	



## Introduction

Effective technical security depends not only on technical measures, but also on appropriate policies and procedures and on good user education and training. The school will be responsible for ensuring that the school infrastructure / network is as safe and secure as is reasonably possible and that:

- users can only access data to which they have right of access
- no user should be able to access another's files (other than that allowed for monitoring purposes within the school's policies).
- access to personal data is securely controlled in line with the school's personal data policy
- logs are maintained of access by users and of their actions while users of the system
- there is effective guidance and training for users
- there are regular reviews and audits of the safety and security of school computer systems
- there is oversight from senior leaders and these have impact on policy and practice.

## Responsibilities

The management of technical security will be the responsibility of Mrs L. Sockett, Miss S. Roscoe & Miss B. Evans

## Technical Security

### Policy statements

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 will receive guidance and training and will be effective in carrying out their responsibilities:

- School technical systems will be managed in ways that ensure that the school meets recommended technical requirements
- There will be regular reviews and audits of the safety and security of school technical systems
- Servers, wireless systems and cabling must be securely located and physical access restricted
- Appropriate security measures are in place to protect the servers, firewalls, switches, routers, wireless systems, work stations, mobile devices etc from accidental or malicious attempts which might threaten the security of the school systems and data.
- Responsibilities for the management of technical security are clearly assigned to appropriate and well trained staff
- All users will have clearly defined access rights to school technical systems. Details of the access rights available to groups of users will be recorded by the Network Manager / Technical Staff / Other person and will be reviewed, at least annually, by the e-Safety Committee (or other group).
- Users will be made responsible for the security of their username and password, must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security. (See Password section below).
- LA and IT Co-ordinator is responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations.
- Mobile device security and management procedures are in place.
- School / Local Authority staff regularly monitor and record the activity of users on the school technical systems and users are made aware of this in the Acceptable Use Agreement.
- An appropriate system is in place for users to report any actual / potential technical incident to the e-Safety Coordinator / Network Manager / Technician (or other relevant person, as agreed).
- An agreed policy is in place for the provision of temporary access of "guests" (eg trainee teachers, supply teachers, visitors) onto the school system.
- An agreed policy is in place regarding the extent of personal use that users (staff / students / pupils / community users) and their family members are allowed on school devices that may be used out of school.

- An agreed policy is in place regarding the use of removable media (eg memory sticks / CDs / DVDs) by users on school devices.
- The school infrastructure and individual workstations are protected by up to date software to protect against malicious threats from viruses, worms, trojans etc.
- Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured.

## **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).

### **Policy Statements:**

- All users will have clearly defined access rights to school technical systems and devices. Details of the access rights available to groups of users will be recorded by the Network Manager (or other person) and will be reviewed, at least annually, by the e-Safety Committee (or other group).
- All school networks and systems will be protected by secure passwords that are regularly changed
- The “master / administrator” passwords for the school systems, used by the technical staff must also be available to the Headteacher or other nominated senior leader and kept in a secure place eg school safe. Consideration should also be given to using two factor authentication for such accounts.
- Passwords for new users, and replacement passwords for existing users will be allocated by IT Co-ordinator via the LA. Any changes carried out must be notified to the manager of the password security policy.
- All users (adults and young people) will have responsibility for the security of their username and password, must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security.
- requests for password changes should be authenticated by (the responsible person) to ensure that the new password can only be passed to the genuine user.

### **Staff passwords:**

- All staff users will be provided with a username and password by the IT Co-ordinator who will keep an up to date record of users and their usernames.
- for best practice, the password should be a minimum of 8 characters long and must include three of – uppercase character, lowercase character, number, special characters
- must not include proper names or any other personal information about the user that might be known by others
- passwords shall not be displayed on screen, and shall be securely hashed (use of one-way encryption)
- passwords should be different for different accounts, to ensure that other systems are not put at risk if one is compromised and should be different for systems used inside and outside of school
- should be different for different accounts, to ensure that other systems are not put at risk if one is compromised
- should be different for systems used inside and outside of school

### **Student / pupil passwords:**

- All users will be provided with a username and password by the IT Co-ordinator who will keep an up to date record of users and their usernames.
- Pupils will be taught the importance of password security
- The complexity (ie minimum standards) will be set with regards to the cognitive ability of the children.

## **Training / Awareness:**

It is essential that users should be made aware of the need for keeping passwords secure, and the risks attached to unauthorised access / data loss. This should apply to even the youngest of users, even if class log-ons are being used.

Members of staff will be made aware of the school's password policy:

- at induction
- through the school's e-Safety policy and password security policy
- through the Acceptable Use Agreement

Students will be made aware of the school's password policy:

- in lessons
- through the Acceptable Use Agreement

## **Audit / Monitoring / Reporting / Review:**

The responsible person (IT Co-ordinator) will ensure that full records are kept of:

- User Ids and requests for password changes
- Security incidents related to this policy

## **Filtering**

### **Introduction**

The filtering of internet content provides an important means of preventing users from accessing material that is illegal or is inappropriate in an educational context. The filtering system cannot, however, provide a 100% guarantee that it will do so, because the content on the web changes dynamically and new technologies are constantly being developed. It is important, therefore, to understand that filtering is only one element in a larger strategy for e-Safety and acceptable use. It is important that the school has a filtering policy to manage the associated risks and to provide preventative measures which are relevant to the situation in this school.

### **Responsibilities:**

The responsibility for the management of the school's filtering policy will be held by (IT Co-ordinator). 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.

To ensure that there is a system of checks and balances and to protect those responsible, changes to the school filtering service must:

- be logged in change control logs
- be reported to a second responsible person (Headteacher) and to be authorised by the second responsible person prior to changes being made

All users have a responsibility to report immediately to (IT Co-ordinator or Headteacher) any infringements of the school's filtering policy of which they become aware or any sites that are accessed, which they believe should have been filtered.

Users must not attempt to use any programmes or software that might allow them to bypass the filtering / security systems in place to prevent access to such materials.

### **Policy Statements:**

Internet access is filtered for all users. Differentiated internet access is available for staff and customised filtering changes are managed by the school. Illegal content is filtered by broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list and other illegal content lists. Filter content lists are regularly updated and internet use is logged and frequently monitored. Ideally, the monitoring process alerts the school to breaches of the filtering policy, which

are then acted upon. There is a clear route for reporting and managing changes to the filtering system. Where personal mobile devices are allowed internet access through the school network, filtering will be applied that is consistent with school practice.

- The school maintains and supports the managed filtering service provided by the Internet Service Provider
- Mobile devices that access the school internet connection (whether school or personal devices) will be subject to the same filtering standards as other devices on the school systems
- Any filtering issues should be reported immediately to the filtering provider.
- Requests from staff for sites to be removed from the filtered list will be considered by the technical staff or Service Provider. If the request is agreed, this action will be recorded and logs of such actions shall be reviewed regularly by the e-Safety Group.

### **Education / Training / Awareness:**

Pupils will be made aware of the importance of filtering systems through the e-Safety education programme. They will also be warned of the consequences of attempting to subvert the filtering system.

Staff users will be made aware of the filtering systems through:

- the Acceptable Use Agreement
- staff meetings, briefings, Inset.

Parents will be informed of the school's filtering policy through the Acceptable Use Agreement and through e-Safety awareness sessions / newsletter etc.

### **Monitoring:**

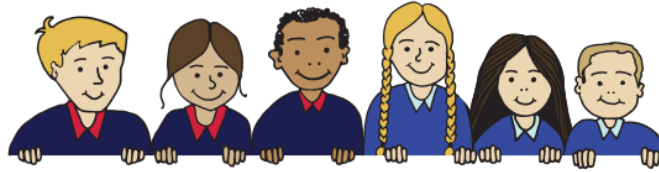
No filtering system can guarantee 100% protection against access to unsuitable sites. The school will therefore monitor the activities of users on the school network and on school equipment as indicated in the School e-Safety Policy and the Acceptable Use Agreement.

### **Audit / Reporting:**

Logs of filtering change controls and of filtering incidents will be made available to:

- the second responsible person (Headteacher)
- e-Safety Group
- e-Safety Governor / Governors committee
- Local Authority / Police on request

The filtering policy will be reviewed in the response to the evidence provided by the audit logs of the suitability of the current provision.



HAPUSRWYDD ▪ HYDER ▪ LLWYDDIANT  
HAPPINESS ▪ CONFIDENCE ▪ SUCCESS



## Ffederasiwn Dyffryn Ceiriog Ceiriog Valley Federation

### School Personal Data Handling Policy

---

#### Introduction

Approved by Governing Body on	Date:
Due for review on	Date: May 2022
Signed by Chair of Governing Body	
(Print name)	

Schools and their employees should do everything within their power to ensure the safety and security of any material of a personal or sensitive nature.

It is the responsibility of all members of the school community to take care when handling, using or transferring personal data that it cannot be accessed by anyone who does not:

- have permission to access that data, and/or
- need to have access to that data.

Data breaches can have serious effects on individuals and / or institutions concerned, can bring the school into disrepute and may well result in disciplinary action, criminal prosecution and fines imposed by the Information Commissioners Office - for the school and the individuals involved. Particularly, all transfer of data is subject to risk of loss or contamination.

Anyone who has access to personal data must know, understand and adhere to this policy, which brings together the legal requirements contained in relevant data protection legislation and relevant regulations and guidance (where relevant from the Local Authority).

*The DPA lays down a set of rules for processing of personal data (both structured manual records and digital records). It provides individuals (data subjects) with rights of access and correction. The DPA requires organisations to comply with eight data protection principles, which, among others require data controllers to be open about how the personal data they collect is used.*

The DPA defines "Personal Data" as data which relate to a living individual who can be identified [http://ico.org.uk/for\\_organisations/data\\_protection/the\\_guide/key\\_definitions](http://ico.org.uk/for_organisations/data_protection/the_guide/key_definitions)

- from those data, or
- from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller,
- and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual.

It further defines "Sensitive Personal Data" as personal data consisting of information as to:

- the racial or ethnic origin of the data subject,
- his political opinions,
- his religious beliefs or other beliefs of a similar nature,
- whether he is a member of a trade union (within the meaning of the Trade Union and Labour Relations (Consolidation) Act 1992),
- his physical or mental health or condition,
- his sexual life,
- the commission or alleged commission by him of any offence, or
- any proceedings for any offence committed or alleged to have been committed by him, the disposal of such proceedings or the sentence of any court in such proceedings.

Guidance for organisations processing personal data is available on the Information Commissioner's Office website: [http://www.ico.gov.uk/for\\_organisations/data\\_protection\\_guide.aspx](http://www.ico.gov.uk/for_organisations/data_protection_guide.aspx)

## Policy Statements

The school 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".

## Personal Data

The school and individuals will have access to a wide range of personal information and data. The data may be held in a digital format or on paper records. Personal data is defined as any combination of data items that identifies an individual and provides specific information about them, their families or circumstances. This will include:

- Personal information about members of the school community – including pupils, members of staff and parents / carers eg names, addresses, contact details, legal guardianship contact details, health records, disciplinary records
- Curricular / academic data eg class lists, pupil / student progress records, reports, references
- Professional records eg employment history, taxation and national insurance records, appraisal records and references
- Any other information that might be disclosed by parents / carers or by other agencies working with families or staff members.

## Responsibilities

The school's Senior Information Risk Officer (SIRO) is **Miss Beth Evans**. This person will keep up to date with current legislation and guidance and will:

- determine and take responsibility for the school's information risk policy and risk assessment
- appoint the Information Asset Owners (IAOs)

The school will identify Information Asset Owners (IAOs) **Mrs L Sockett** for the various types of data being held (eg pupil / student information / staff information / assessment data etc). The IAOs will manage and address risks to the information and will understand:

- what information is held, for how long and for what purpose,
- how information has been amended or added to over time, and
- who has access to protected data and why.

Everyone in the school has the responsibility of handling protected or sensitive data in a safe and secure manner.

Governors are required to comply fully with this policy in the event that they have access to personal data, when engaged in their role as a Governor.

## Registration

The school is registered as a Data Controller on the Data Protection Register held by the Information Commissioner. **(All schools complete an annual form):**

[http://www.ico.gov.uk/what\\_we\\_cover/register\\_of\\_data\\_controllers.aspx](http://www.ico.gov.uk/what_we_cover/register_of_data_controllers.aspx)

## Information to Parents / Carers – the “Privacy Notice”

In order to comply with the fair processing requirements of the DPA, the school will inform parents / carers of all pupils / students of the data they collect, process and hold on the pupils / students, the purposes for which the data is held and the third parties (eg LA, DfE, etc) to whom it may be passed. This privacy notice will be passed to parents / carers through parent's pack, reports or a specific letter / communication. Parents / carers of young people who are new to the school will be provided with the privacy notice through letter.

## Training & awareness

All staff will receive data handling awareness / data protection training and will be made aware of their responsibilities, as described in this policy through:

- Induction training for new staff
- Staff meetings / briefings / Inset
- Day to day support and guidance from Administration

## Risk Assessments

Information risk assessments will be carried out by Information Asset Owners (Admin) to establish the security measures already in place and whether they are the most appropriate and cost effective. The risk assessment will involve:

- Recognising the risks that are present;
- Judging the level of the risks (both the likelihood and consequences); and
- Prioritising the risks.

Risk assessments are an ongoing process and should result in the completion of an Information Risk Actions Form (example below):

Risk ID	Information Asset affected	Information Asset Owner	Protective Marking (Impact Level)	Likelihood	Overall risk level (low, medium, high)	Action(s) to minimise risk

## Impact Levels and protective marking

Following incidents involving loss of data, the Government recommends that the Protective Marking Scheme should be used to indicate the sensitivity of data. The Protective Marking Scheme is mapped to Impact Levels as follows:

Government Protective Marking Scheme label	Impact Level (IL)	Applies to schools?
NOT PROTECTIVELY MARKED	0	Will apply in schools
PROTECT	1 or 2	
RESTRICTED	3	
CONFIDENTIAL	4	Will not apply in schools
HIGHLY CONFIDENTIAL	5	
TOP SECRET	6	

Most pupil or staff personal data that is used within educational institutions will come under the PROTECT classification. However some, eg the home address of a child (or vulnerable adult) at risk will be marked as RESTRICT.

The school will ensure that all school staff, independent contractors working for it, and delivery partners, comply with restrictions applying to the access to, handling and storage of data classified as Protect, Restricted or higher. Unmarked material is considered 'unclassified'. The term



'UNCLASSIFIED' or 'NON' or 'NOT PROTECTIVELY MARKED' may be used to indicate positively that a protective marking is not needed.

All documents (manual or digital) that contain protected or restricted data will be labelled clearly with the Impact Level shown in the header and the Release and Destruction classification in the footer.

Users must be aware that when data is aggregated the subsequent impact level may be higher than the individual impact levels of the original data. Combining more and more individual data elements together in a report or data view increases the impact of a breach. A breach that puts students / pupils at serious risk of harm will have a higher impact than a risk that puts them at low risk of harm. Long-term significant damage to anyone's reputation has a higher impact than damage that might cause short-term embarrassment.

Release and destruction markings should be shown in the footer eg. "Securely delete or shred this information when you have finished using it".

## Secure Storage of and access to data

The school will ensure that ICT systems are set up so that the existence of protected files is hidden from unauthorised users and that users will be assigned a clearance that will determine which files are accessible to them. Access to protected data will be controlled according to the role of the user. Members of staff will not, as a matter of course, be granted access to the whole management information system.

All users will use strong passwords. User passwords must never be shared.

Personal data may only be accessed on machines that are securely password protected. Any device that can be used to access data must be locked if left (even for very short periods) and set to auto lock if not used for five minutes.

All storage media must be stored in an appropriately secure and safe environment that avoids physical risk, loss or electronic degradation.

Personal data can only be stored on school equipment (this includes computers and portable storage media. Private equipment (ie owned by the users) must not be used for the storage of personal data.

When personal data is stored on any portable computer system, USB stick or any other removable media:

- 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 (below) once it has been transferred or its use is complete.

The school has clear policy and procedures for the automatic backing up, accessing and restoring all data held on school systems, including off-site backups.

The school has clear policy and procedures for the use of "Cloud Based Storage Systems" (for example Office365) and is aware that data held in remote and cloud storage is still required to be protected in line with the Data Protection Act. The school will ensure that it is satisfied with controls put in place by remote / cloud based data services providers to protect the data.  
[http://www.ico.org.uk/for\\_organisations/guidance\\_index/~media/documents/library/Data\\_Protection/Practical\\_application/cloud\\_computing\\_guidance\\_for\\_organisations.ashx](http://www.ico.org.uk/for_organisations/guidance_index/~media/documents/library/Data_Protection/Practical_application/cloud_computing_guidance_for_organisations.ashx)

As a Data Controller, the school is responsible for the security of any data passed to a "third party". Data Protection clauses will be included in all contracts where data is likely to be passed to a third party.

All paper based Protected and Restricted (or higher) material must be held in lockable storage, whether on or off site.

The school recognises that under Section 7 of the DPA, <http://www.legislation.gov.uk/ukpga/1998/29/section/7> data subjects have a number of rights in connection with their personal data, the main one being the right of access. Procedures are in place to deal with Subject Access Requests i.e. a written request to see all or a part of the personal data held by the data controller in connection with the data subject. Data subjects have the right to know: if the data controller holds personal data about them; a description of that data; the purpose for which the data is processed; the sources of that data; to whom the data may be disclosed; and a copy of all the personal data that is held about them. Under certain circumstances the data subject can also exercise rights in connection with the rectification; blocking; erasure and destruction of data.

## Secure transfer of data and access out of school

The school recognises that personal data may be accessed by users out of school, or transferred to the LA or other agencies. In these circumstances:

- Users may not remove or copy sensitive or restricted or protected personal data from the school or authorised premises without permission and unless the media is encrypted and password protected and is transported securely for storage in a secure location.
- Users must take particular care that computers or removable devices which contain personal data must not be accessed by other users (eg family members) when out of school
- When restricted or protected personal data is required by an authorised user from outside the organisation's premises (for example, by a member of staff to work from their home), they should preferably have secure remote access to the management information system or learning platform;
- If secure remote access is not possible, users must only remove or copy personal or sensitive data from the organisation or authorised premises if the storage media, portable or mobile device is encrypted and is transported securely for storage in a secure location;
- Users must protect all portable and mobile devices, including media, used to store and transmit personal information using approved encryption software; and
- Particular care should be taken if data is taken or transferred to another country, particularly outside Europe, and advice should be taken from the local authority in this event.

## Disposal of data

The school will comply with the requirements for the safe destruction of personal data when it is no longer required.

The disposal of personal data, in either paper or electronic form, must be conducted in a way that makes reconstruction highly unlikely. Electronic files must be securely overwritten, in accordance with government guidance, and other media must be shredded, incinerated or otherwise disintegrated for data.

A Destruction Log should be kept of all data that is disposed of. The log should include the document ID, classification, date of destruction, method and authorisation.

## Audit Logging / Reporting / Incident Handling

It is good practice, as recommended in the "Data Handling Procedures in Government" document that the activities of data users, in respect of electronically held personal data, will be logged and these logs will be monitored by responsible individual-Mrs M Lewis Administration. The audit logs will be kept to provide evidence of accidental or deliberate data security breaches – including loss of protected data or breaches of an acceptable use policy, for example.

The school has a **procedures for reporting, managing and recovering from information risk incidents**, which establishes:

- a "responsible person" for each incident;
- a communications plan, including escalation procedures;
- and results in a plan of action for rapid resolution; and

- a plan of action of non-recurrence and further awareness raising.

All significant data protection incidents must be reported through the SIRO to the Information Commissioner's Office based upon the local incident handling policy and communication plan

## Use of technologies and Protective Marking

The following provides a useful guide:

	<b>The information</b>	<b>The technology</b>	<b>Notes on Protect Markings (Impact Level)</b>
<b>School life and events</b>	School terms, holidays, training days, the curriculum, extra-curricular activities, events, displays of pupils work, lunchtime menus, extended services, parent consultation events	Common practice is to use publically accessible technology such as school websites or portal, emailed newsletters, subscription text services	Most of this information will fall into the NOT PROTECTIVELY MARKED (Impact Level 0) category.
<b>Learning and achievement</b>	Individual pupil / student academic, social and behavioural achievements, progress with learning, learning behaviour, how parents can support their child's learning, assessments, attainment, attendance, individual and personalised curriculum and educational needs.	Typically schools will make information available by parents logging on to a system that provides them with appropriately secure access, such as a Learning Platform or portal, or by communication to a personal device or email account belonging to the parent.	Most of this information will fall into the PROTECT (Impact Level 2) category. There may be students/ pupils whose personal data requires a RESTRICTED marking (Impact Level 3) or higher. For example, the home address of a child at risk. In this case, the school may decide not to make this pupil / student record available in this way.
<b>Messages and alerts</b>	Attendance, behavioural, achievement, sickness, school closure, transport arrangements, and other information that it may be important to inform or contact a parent about as soon as possible. This may be particularly important when it is necessary to contact a parent concerning information that may be considered too sensitive to make available using other online means.	Email and text messaging are commonly used by schools to contact and keep parents informed. Where parents are frequently accessing information online then systems e.g. Learning Platforms or portals, might be used to alert parents to issues via "dashboards" of information, or be used to provide further detail and context.	Most of this information will fall into the PROTECT (Impact Level 1) category. However, since it is not practical to encrypt email or text messages to parents, schools should not send detailed personally identifiable information. General, anonymous alerts about schools closures or transport arrangements would fall into the NOT PROTECTIVELY MARKED (Impact Level 0) category.

## Appendices: Additional issues / documents related to Personal Data Handling in Schools:

## Use of Cloud Services

The movement towards tablet and other mobile technologies in schools presents both opportunities as well as challenges. Ultimately, the opportunities are around teaching and learning; the challenges are around successfully managing this pedagogical shift and taking staff, parents and pupils through this technological change. At the heart of the change is a move away from devices or systems where information is stored locally, to devices which can access data stored 'in the cloud'. Just as a PC needs to be connected to a network to get to the stored data, so must these mobile and tablet devices be connected to the cloud. Wireless access provides this connection.

Software too can sit in the cloud removing the need for locally installed suites of software. Apps offer an opportunity to create low cost, flexible learning opportunities which are device agnostic and which can create personalised learning on a new level.

Schools using the Hwb+ learning platform will have been provisioned with Office 365 which offers cloud based email, calendar and storage facilities as well as MS Office. By its nature, Office 365 is available on any device which is connected to the internet meaning that these cloud based services can be accessed in school or at home on smartphones, tablets, laptops, notebooks and PCs. Schools may wish to encourage a Bring Your Own Device (BYOD) approach which will require as a minimum a strengthening of the existing Acceptable Use Policy/Agreement.

Just as a school has obligations around data on its physical network, the same obligations are required when dealing with data in the cloud i.e. it is still required to be protected in line with the Data Protection Act (DPA) and may be subject to Freedom of Information (FOI) requests.

## Freedom of Information

FOI may require anything you write in an official capacity to be potentially made public. This might mean you need to consider how long content is stored for and the ease of which it can be recovered from a cloud archive.

Cloud services very often are not designed for the long term storage of content, particularly transient communications with high volume like email. Schools should consider how to secure and back-up to a local system what could be sensitive or important data.

A summary of good practice in dealing with requests can be found [here](#)

## Data Protection Act

Schools, like any other organisation, are subject to the Data Protection Act (DPA) and its eight basic principles. The DPA refers to 'personal data' – this can be described generally as information which identifies an individual and is personal to an individual.

The DPA contains eight 'Data Protection Principles' which specify that personal data must be:

- Processed fairly and lawfully
- Obtained for specified and lawful purposes
- Adequate, relevant and not excessive
- Accurate and up to date
- Not kept any longer than necessary
- Processed in accordance with the 'data subject's' (the individual's) rights
- Securely kept
- Not transferred to any other country without adequate protection

It's also worth considering that whilst not all data is 'personal', the information that is, has varying levels of sensitivity based on the impact were it to be compromised.

The Information Commissioners Office has produced a report aimed at helping schools meet their data protection obligations; you can read the report detailing data protection advice for schools [here](#) and a simple summary of the report [here](#).

## Safeguarding

There are also safeguarding obligations for the use of technology in schools that include (possibly in partnership with your service provider):

- Effectively monitoring the use of systems to detect potential and actual safeguarding issues
- Monitoring, alerting and responding to illegal activity
- Providing consistent safeguarding provision both within and beyond school if devices/services leave the site

## **Criminal Activity**

Schools have an immediate obligation to report illegal or criminal activity to the Police. A detailed summary of legislation that pertains to safeguarding and schools which can be found elsewhere in this documentation.

Other services e.g. Facebook, Twitter, etc are useful cloud tools in and beyond the classroom but it is important to be aware of age restrictions here too. US Law requires any company operating within the US to comply with the Children's Online Privacy Protection Act (COPPA) which legislates against companies who store, process and manage information on children aged 13 and under and the active or targeted marketing to that age group.

## **Where is the cloud?**

Most education systems have to make use of personal information to function. The DPA (Principle 8) states that personal data must not be transferred to any other country without adequate protection in situ. Data protection requirements vary widely across the globe. Countries in the EU approach privacy protection differently to those outside and are more stringent in the detail and responsibilities of data users than perhaps the US. Microsoft Office 365 is held in data centres in Amsterdam and Dublin.

## **Security concerns**

Can anyone access data in the cloud centre where it sits? Data centres are required to have stringent physical interventions in place against data being compromised from internal or external access. There are sophisticated security mechanisms in place to prevent external hacking of data. Whilst this cannot always be guaranteed to be 100% safe, this sophistication is often beyond the local capability of a single school and so can be regarded as reasonable duty of care.

Access to data through devices is much more likely given that devices are going to and from school in bags, on buses, or left lying around at home or school so security now becomes much more of an issue at a user level than it ever has before. If a device goes missing or breaks, the big advantage of cloud systems is that, apart from simple local settings, content is in the cloud so data is not 'lost' in the same way as if your laptop was stolen or suffers a hard drive failure. Cloud services can offer device management systems that can lock or locate a device if missing.

Passwords and authentication are critical at any point in securing access to data but are especially so with data in the cloud. Some points to consider are:

- Are passwords strong?
- Do users know what a strong password looks like?
- Do you insist on rolling user passwords regularly? Every 60 days? Many businesses do as good practice.
- Are users educated in good password practice? Is this backed up with a clear and reliable password policy?

If you need a template then one can be found as part of this policy suite.

It's also important to ensure there is a clear and reliable culture around reporting issues such as compromise, loss or unethical practice. This doesn't happen on its own and needs to be taught. Again, the common sense, everyday good practice around logging out of systems when finished, having a management plan in place if something goes wrong, and having reporting mechanisms in place also applies to using cloud technologies.

For example, South West Grid for Learning have produced a free Digital Literacy and Citizenship Curriculum for Foundation Stage to Year 10+ which has a variety of strands one of which focuses on Privacy and Security. Pupils and students learn strategies for managing their online information and keeping it secure from online risks such as identity thieves and phishing. They learn how to create

strong passwords, how to avoid scams and schemes, and how to analyse privacy policies. The version of this resource for Wales is available via Hwb (November 2014).

## Monitoring users

Local networks based on site have the advantage of being relatively easy to filter and monitor for inappropriate or illegal use and many schools will already have these systems in place. Filtering can be provided as part of a school's internet provision, particularly if they have that service delivered through the local/unitary authority. A school may choose to provide its own through a variety of commercial solutions.

However, when services move into a wider cloud-based environment hosted by an external partner it becomes more difficult to know what users are storing or accessing, particularly if their connectivity away from the school is a domestic one.

With all of those separate user folders and portfolios with their separate passwords and widely varying content, how can you be sure they are not being used to store inappropriate materials? Illegal materials? The school provides the tools e.g. Office 365 and there is therefore an expectation that the school should ensure that users are operating in a space that is safe as can be created.

Microsoft state in their user agreements that they reserve the right to actively search stored files. This means that the school also needs to be clear about what the expectations are around illegal and inappropriate content and how it intends to ensure those expectations are met. These might include:

- Clear and effective agreement through an Acceptable Use Policy or computer splash screen with "agree" button
- Positive statements around the use of technology dotted around areas where that technology might be used (particularly effective are student-designed posters)
- Active education in raising awareness of what illegal or inappropriate both mean
- Staff development in recognising and escalating reports of illegal content
- Reminders that Cloud Service Providers can and do scan content stored on their servers and that an archive exists
- Establish regular spot checks on mobile devices and advertise the fact that these will be carried out on school devices and removable media
- Establish and communicate that One Drives provided as part of a school cloud solution will be subject to random spot checks by resetting passwords back to default to allow auditing or set the expectation that users should share their online folders with their teacher. The system has been provided for educational use so there should not be anything in there that isn't related to learning.

## Managing accounts and users

Dealing with one tablet or smartphone on your own account is empowering; you can make choices about how you set it up, the apps you want; the subscriptions you choose and how many photos or documents to store on it. Setting up tens of devices with potentially hundreds of users has a whole different set of considerations:

- The distribution and timetabling of school owned devices (particularly those that go home?)
- Can users store content locally on the tablet eg photos?
- Can school network and connectivity sustain the use of many devices?
- Is there one standard profile for everyone or can each user customise?
- How are those profiles managed or swapped?
- Are personal devices allowed to be commissioned to the school system (BYOD)?

A Mobile Device Management layer can be critical in establishing access rights to these technologies. You may need to consult with your service provider to investigate what options are available to you.

## If things go wrong

Like any other safeguarding issue there must be clear and rigorous incident management practice that is consistent with other safeguarding policy.

- Clear and well communicated policy

- Effective routines for securing and recording evidence
- Established reporting routes that are well-communicated, respected and agreed by all
- Clearly communicated sanctions that have been agreed and shared with all users
- Audit trails that are used to shape interventions and inform future practice

## **What policies and procedures should be put in place for individual users of cloud-based services?**

The school is ultimately responsible for the contract with the provider of the system.

Appendix C6 provides a useful summary of issues around Office 365 written with the support of Microsoft:

The document focusses on Office 365, but poses important considerations if a school is considering services from another provider.

## **Privacy and Electronic Communications**

Schools should be aware that the Privacy and Electronic Communications Regulations have changed and that they are subject to these changes in the operation of their websites.

## **Freedom of Information Act**

All schools must have a Freedom of Information Policy which sets out how it will deal with FOI requests. In this policy the school should:

- Delegate to the Headteacher / Principal day-to-day responsibility for FOIA policy and the provision of advice, guidance, publicity and interpretation of the school's policy.
- Consider designating an individual with responsibility for FOIA, to provide a single point of reference, coordinate FOIA and related policies and procedures, take a view on possibly sensitive areas and consider what information and training staff may need.
- Consider arrangements for overseeing access to information and delegation to the appropriate governing body.
- Proactively publish information with details of how it can be accessed through a Publication Scheme (see Model Publication Scheme below) and review this annually.
- Ensure that a well managed records management and information system exists in order to comply with requests.
- Ensure a record of refusals and reasons for refusals is kept, allowing the Academy Trust to review its access policy on an annual basis.

## **Model Publication Scheme**

The Information Commissioners Office provides schools with a model publication scheme which they should complete. This was revised in 2009, so any school with a scheme published prior to then should review this as a matter of urgency. The school's publication scheme should be reviewed annually.

Guidance on the model publication scheme can be found at:

[http://www.ico.gov.uk/for\\_organisations/freedom\\_of\\_information/guide/publication\\_scheme.aspx](http://www.ico.gov.uk/for_organisations/freedom_of_information/guide/publication_scheme.aspx)

The Schools Model Publication Scheme Template is available from:

[http://www.ico.gov.uk/upload/documents/library/freedom\\_of\\_information/detailed\\_specialist\\_guides/schools\\_england\\_mps\\_final.pdf](http://www.ico.gov.uk/upload/documents/library/freedom_of_information/detailed_specialist_guides/schools_england_mps_final.pdf)

## **Further Guidance**

ICO guidance can be found at the following link - including a pdf version - updated in September 2012:

[http://www.ico.gov.uk/for\\_organisations/freedom\\_of\\_information/guide.aspx](http://www.ico.gov.uk/for_organisations/freedom_of_information/guide.aspx)



HAPUSRWYDD ▪ HYDER ▪ LLWYDDIANT  
HAPPINESS ▪ CONFIDENCE ▪ SUCCESS



## School e-Safety Group

### Terms of Reference

#### 1. PURPOSE

To provide a consultative group that has wide representation from the Ceiriog Valley Federation community, with responsibility for issues regarding e-Safety and the monitoring the e-Safety policy including the impact of initiatives. The group will also be responsible for regular reporting to the Full Governing Body.

#### 2. MEMBERSHIP

2.1 The e-Safety committee will seek to include representation from all stakeholders. The composition of the group should include:

- SLT member/s
- Safeguarding officer
- Teaching staff member
- Support staff member
- e-Safety coordinator (not ICT coordinator by default)
- Governor
- Pupil representation – for advice and feedback. *(Pupil voice is essential in the make up of the e-Safety committee, but pupils would only be expected to take part in committee meetings where deemed relevant.)*

2.2 Other people may be invited to attend the meetings at the request of the Chairperson on behalf of the committee to provide advice and assistance where necessary.

2.3 Committee members must declare a conflict of interest if any incidents being discussed directly involve themselves or members of their families.

2.4 Committee members must be aware that many issues discussed by this group could be of a sensitive or confidential nature

2.5 When individual members feel uncomfortable about what is being discussed they should be allowed to leave the meeting with steps being made by the other members to allow for these sensitivities

#### 3. CHAIRPERSON

The Committee should select a suitable Chairperson from within the group. Their responsibilities include:

- Scheduling meetings and notifying committee members;
- Inviting other people to attend meetings when required by the committee;
- Guiding the meeting according to the agenda and time available;
- Ensuring all discussion items end with a decision, action or definite outcome;
- Making sure that notes are taken at the meetings and that these with any action points are



distributed as necessary

#### 4. DURATION OF MEETINGS

Meetings shall be held yearly. A special or extraordinary meeting may be called when and if deemed necessary.

#### 5. FUNCTIONS

These are to assist the e-Safety Co-ordinator (or other relevant person) with the following:

- To keep up to date with new developments in the area of e-Safety
- To (at least) annually review and develop the e-Safety policy in line with new technologies and incidents
- To monitor the delivery and impact of the e-Safety policy
- To monitor the log of reported e-Safety incidents (anonymous) to inform future areas of teaching / learning / training.
- To co-ordinate consultation with the whole school community to ensure stakeholders are up to date with information, training and/or developments in the area of e-Safety. This could be carried out through[add/delete as relevant]:
  - Staff meetings
  - Student / pupil forums (for advice and feedback)
  - Governors meetings
  - Surveys/questionnaires for students / pupils, parents / carers and staff
  - Parents evenings
  - Website/VLE/Newsletters
  - e-Safety events
  - Internet Safety Day (annually held on the second Tuesday in February)
  - Other methods
- To ensure that monitoring is carried out of Internet sites used across the school (if possible)
- To monitor filtering / change control logs (e.g. requests for blocking / unblocking sites).
- To monitor the safe use of data across the Federation.
- To monitor incidents involving cyberbullying for staff and pupils

#### 6. AMENDMENTS

The terms of reference shall be reviewed annually from the date of approval. They may be altered to meet the current needs of all committee members, by agreement of the majority.

The above Terms of Reference for the schools of Ceiriog Valley Federation have been agreed

Signed by (SLT):

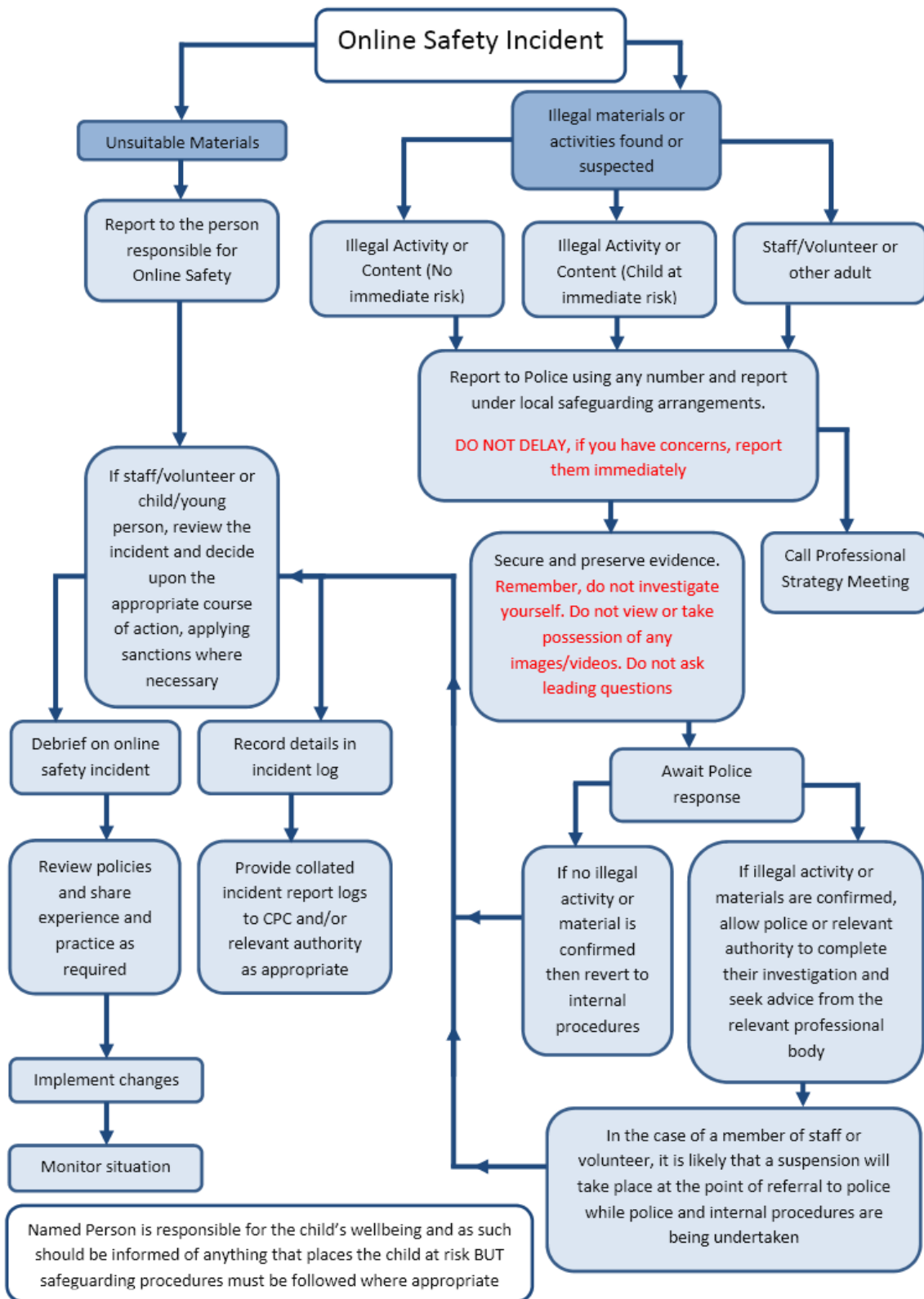
Date:

Date for review:

#### Acknowledgement

This template terms of reference document is based on one provided to schools by Wrexham County Council.

# Responding to incidents of misuse – flow chart



## Record of reviewing devices / internet sites (responding to incidents of misuse)

Group	
Date	
Reason for investigation	

**Details of first reviewing person**

Name	
Position	
Signature	

**Details of second reviewing person**

Name	
Position	
Signature	

**Name and location of computer used for review (for web sites)**

--

<b>Web site(s) address / device</b>	<b>Reason for concern</b>
-------------------------------------	---------------------------


**Conclusion and Action proposed or taken**


C3


## Reporting Log

Reporting Log Group .....	Date	Time	Incident	Action taken		Incident Reported by	Signature
				What?	By whom?		

C4

## Training Needs Audit

Training Needs Audit Log Group .....		Date .....							
Name	Position	Relevant training in last 12 months	Identified training need	To be met by:	Cost	Review date			

## Summary of Legislation

Schools should be aware of the legislative framework under which this e-Safety Policy template and guidance has been produced. It is important to note that in general terms an action that is illegal if committed offline is also illegal if committed online.

It is recommended that legal advice is sought in the advent of an e safety issue or situation.

### Computer Misuse Act 1990

This Act makes it an offence to:

- Erase or amend data or programs without authority;
- Obtain unauthorised access to a computer;
- “Eavesdrop” on a computer;
- Make unauthorised use of computer time or facilities;
- Maliciously corrupt or erase data or programs;
- Deny access to authorised users.

### Data Protection Act 1998

This protects the rights and privacy of individual’s data. To comply with the law, information about individuals must be collected and used fairly, stored safely and securely and not disclosed to any third party unlawfully. The Act states that person data must be:

- Fairly and lawfully processed.
- Processed for limited purposes.
- Adequate, relevant and not excessive.
- Accurate.
- Not kept longer than necessary.
- Processed in accordance with the data subject’s rights.
- Secure.
- Not transferred to other countries without adequate protection.

### Freedom of Information Act 2000

The Freedom of Information Act gives individuals the right to request information held by public authorities. All public authorities and companies wholly owned by public authorities have obligations under the Freedom of Information Act. When responding to requests, they have to follow a number of set procedures.

### Communications Act 2003

Sending by means of the Internet a message or other matter that is grossly offensive or of an indecent, obscene or menacing character; or sending a false message by means of or persistently making use of the Internet for the purpose of causing annoyance, inconvenience or needless anxiety is guilty of an offence liable, on conviction, to imprisonment. This wording is important because an offence is complete as soon as the message has been sent: there is no need to prove any intent or purpose.

### Malicious Communications Act 1988

It is an offence to send an indecent, grossly offensive, or threatening letter, electronic communication or other article to another person. It is also an offence to send information which is false and known or believed to be false by the sender.

### Regulation of Investigatory Powers Act 2000

It is an offence for any person to intentionally and without lawful authority intercept any communication. Where the system controller has given express consent monitoring or keeping a record of any form of electronic communications is permitted, in order to:

- Establish the facts;
- Ascertain compliance with regulatory or self-regulatory practices or procedures;
- Demonstrate standards, which are or ought to be achieved by persons using the system;
- Investigate or detect unauthorised use of the communications system;
- Prevent or detect crime or in the interests of national security;
- Ensure the effective operation of the system.
- Monitoring but not recording is also permissible in order to:
- Ascertain whether the communication is business or personal;
- Protect or support help line staff.

### **Trade Marks Act 1994**

This provides protection for Registered Trade Marks, which can be any symbol (words, shapes or images) that are associated with a particular set of goods or services. Registered Trade Marks must not be used without permission. This can also arise from using a Mark that is confusingly similar to an existing Mark.

### **Copyright, Designs and Patents Act 1988**

It is an offence to copy all, or a substantial part of a copyright work. There are, however, certain limited user permissions, such as fair dealing, which means under certain circumstances permission is not needed to copy small amounts for non-commercial research or private study. The Act also provides for Moral Rights, whereby authors can sue if their name is not included in a work they wrote, or if the work has been amended in such a way as to impugn their reputation. Copyright covers materials in print and electronic form, and includes words, images, and sounds, moving images, TV broadcasts and other media (e.g. youtube).

### **Criminal Justice & Public Order Act 1994 / Public Order Act 1986**

This defines a criminal offence of intentional harassment, which covers all forms of harassment, including sexual. A person is guilty of an offence if, with intent to cause a person harassment, alarm or distress, they:

- Use threatening, abusive or insulting words or behaviour, or disorderly behaviour; or
- Display any writing, sign or other visible representation, which is threatening, abusive or insulting, thereby causing that or another person harassment, alarm or distress.

### **Racial and Religious Hatred Act 2006 / Public Order Act 1986**

This Act makes it a criminal offence to threaten people because of their faith, or to stir up religious hatred by displaying, publishing or distributing written material which is threatening. Other laws already protect people from threats based on their race, nationality or ethnic background.

### **Protection from Harassment Act 1997**

A person must not pursue a course of conduct, which amounts to harassment of another, and which he knows or ought to know amounts to harassment of the other. A person whose course of conduct causes another to fear, on at least two occasions, that violence will be used against him is guilty of an offence if he knows or ought to know that his course of conduct will cause the other so to fear on each of those occasions.

### **Protection of Children Act 1978**

It is an offence to take, permit to be taken, make, possess, show, distribute or advertise indecent images of children in the United Kingdom. A child for these purposes is anyone under the age of 18. An image of a child also covers pseudo-photographs (digitally collated or otherwise). A person convicted of such an offence is liable to imprisonment for a term of not more than 10 years, or to a fine or to both.

### **Sexual Offences Act 2003**

The new grooming offence is committed if you are over 18 and have communicated with a child under 16 at least twice (including by phone or using the Internet) it is an offence to meet them or travel to meet them anywhere in the world with the intention of committing a sexual offence. Causing a child under 16 to watch a sexual act is illegal, including looking at images such as videos, photos or webcams, for your own gratification. It is also an offence for a person in a position of trust to engage in sexual activity with any person under 18, with whom they are in a position of trust. (Typically, teachers, social workers, health professionals, connexions staff fall in this category of trust). Any sexual intercourse with a child under the age of 13 commits the offence of rape.

### **Public Order Act 1986**

This Act makes it a criminal offence to stir up racial hatred by displaying, publishing or distributing written material which is threatening. Like the Racial and Religious Hatred Act 2006 it also makes the possession of inflammatory material with a view of releasing it a criminal offence.

### **Obscene Publications Act 1959 and 1964**

Publishing an “obscene” article is a criminal offence. Publishing includes electronic transmission.

### **Human Rights Act 1998**

This does not deal with any particular issue specifically or any discrete subject area within the law. It is a type of “higher law”, affecting all other laws. In the school context, human rights to be aware of include:

- The right to a fair trial
- The right to respect for private and family life, home and correspondence
- Freedom of thought, conscience and religion
- Freedom of expression
- Freedom of assembly
- Prohibition of discrimination
- The right to education
- The right not to be subjected to inhuman or degrading treatment or punishment

The school is obliged to respect these rights and freedoms, but should balance them against those rights, duties and obligations, which arise from other relevant legislation.

### **The Education and Inspections Act 2006**

Empowers Headteachers, to such extent as is reasonable, to regulate the behaviour of students / pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour.

### **The Protection of Freedoms Act 2012**

Requires schools to seek permission from a parent / carer to use Biometric systems



## Office 365 – further information

### Where is the data stored?

Data for UK Schools is all hosted within the EU. The primary Microsoft data centre we host the service in is located in Dublin and the fail-over is to Amsterdam.

### How often is the data backed up?

The idea of “back up” is very different with Office365 than with traditional locally hosted services. We use a network of globally redundant data centres and replicate data on multiple servers across the two data centres. Any one time we keep 3 copies of schools data across the two data-centres mentioned (Dublin & Amsterdam).

### Does the email service provider have a clear process for recovering data?

Yes. Users themselves can recover data for 30 days after deleting an item. Administrators then have a further 30 days once the item is deleted from the deleted-items folder. There are also additional paid-for archiving services available with Office365, but with a 25GB inbox per person the pressure on users to archive email is not as great compared to existing email systems.

### How does the email provider protect your privacy?

3 key things: No advertising, no “mingling” of Office 365 data with our consumer services (such as Hotmail) and full data-portability, in case you ever want to leave the service.

### Who owns the data that you store on the email platform?

Schools own the data. Microsoft does not. You own your data, and retain all rights, title and interest in the data you store with Office 365. You can download a copy of all of your data at any time and for any reason, without any assistance from Microsoft.

### Who has access to the data?

By default no one has access to customer data within the Office 365 service. Microsoft employees who have completed appropriate background checks and have justified need can raise an escalation for time-limited access to Customer data. Access is regularly audited, logged and verified through the ISO 27001 Certification.

As detailed in a recent accreditation submission to the UK Government, any organisation that specify “UK” as their country during tenant creation will be provisioned and data stored within the EU datacenters (Dublin and Amsterdam).

Microsoft has been granted accreditation up to and including the UK government’s “Impact Level 2” (IL2) assurance for Office 365. As of February 2013 Microsoft are the only major international public cloud service provider to have achieved this level of accreditation and, indeed, it is the highest level of accreditation possible with services hosted outside of the UK (but inside of the EEA).

Schools may wish to consider the extent to which applicable laws in the US – which apply to services operated by companies registered in the US, e.g. Microsoft and Google – affect the suitability of these services. For

example the US Patriot Act provides a legal means through which law enforcement agencies can access data held within these services without necessarily needing the consent or even the knowledge of the customer. Whilst SWGfL doesn’t intend to put anyone off getting value from these beneficial services we feel it’s only right to share what we know about them.

### Is personal information shared with anyone else?

No personal information is shared.

**Does the email provider share email addresses with third party advertisers? Or serve users with ads?**

No. There is no advertising in Office365.

**What steps does the email provider take to ensure that your information is secure?**

Microsoft uses 5 layers of security - data, application, host, network and physical. You can read about this in a lot more detail here.

Office365 is certified for ISO 27001, one of the best security benchmarks available across the world. Office 365 was the first major business productivity public cloud service to have implemented the rigorous set of physical, logical, process and management controls defined by ISO 27001.

EU Model Clauses. In addition to EU Safe Harbor, Office 365 is the first major business productivity public cloud service provider to sign the standard contractual clauses created by the European Union ("EU Model Clauses") with all customers. EU Model Clauses address international transfer of data.

Data Processing Agreement. Microsoft offers a comprehensive standard Data Processing Agreement (DPA) to all customers. DPA addresses privacy, security and handling of customer data. Our standard Data Processing Agreement enables customers to comply with their local regulations. Visit here to get a signed copy of the DPA.

**How reliable is the email service?**

There is a 99.9% uptime commitment with financially-backed SLA for any paid-for services in Office365 (though most schools will be using 'free' services and therefore will not receive the financially backed SLA).

**What level of support is offered as part of the service?**

Microsoft offer schools direct telephone support 24/7 for IT administrators and there is also a large range of online help services, which you can read about here. Our recommendation is that schools use a Microsoft partner or support organisation with industry specific expertise in cloud services for schools.

**Additional Resources**

There is a wealth of information about Office365 in the Office365 Trust Centre. You can also read articles about Office365, get deployment resources and contact Microsoft Cloud experts direct on their [UK Schools Cloud Blog](#).

## Glossary of terms

AUP	Acceptable Use Policy – see templates earlier in this document
CEOP	Child Exploitation and Online Protection Centre (part of UK Police, dedicated to protecting children from sexual abuse, providers of the Think U Know programmes.
CPD	Continuous Professional Development
CYPS	Children and Young Peoples Services (in Local Authorities)
FOSI	Family Online Safety Institute
EA	Education Authority
ICO	Information Commissioners Office
ICT	Information and Communications Technology
ICTMark	Quality standard for schools provided by NAACE
INSET	In Service Education and Training
IP address protocol)	The label that identifies each computer to other computers using the IP (internet
ISP	Internet Service Provider
ISPA	Internet Service Providers' Association
IWF	Internet Watch Foundation
LA	Local Authority
LAN	Local Area Network
MIS	Management Information System
NEN	National Education Network – works with the Regional Broadband Consortia (e.g. SWGfL) to provide the safe broadband provision to schools across Britain.
Ofcom	Office of Communications (Independent communications sector regulator)
SWGfL	South West Grid for Learning Trust – the Regional Broadband Consortium of SW Local Authorities – is the provider of broadband and other services for schools and other organisations in the SW
TUK parents.	Think U Know – educational e-Safety programmes for schools, young people and
VLE	Virtual Learning Environment (a software system designed to support teaching and learning in an educational setting.
WAP	Wireless Application Protocol