|  |  |
| --- | --- |
| **THE SCHOOL AT THE HEART OF WALES****ONLINE SAFETY POLICY** |  |



#

#

|  |  |
| --- | --- |
| **Date adopted** | **September 2022** |
| **Signature of Headteacher** |  |
| **Signature of chair of governors** |  |
| **Review Date**  | **September 2023** |

# Diogelwch Ar Lein / Online Safety

**Awdur/Author:** L.Jones

**Adran/Department:** Whole School

**Dyddiad/Date:** 16 November 2021

|  |  |
| --- | --- |
| Builth Wells CampusCollege Rd, Builth Wells, Powys, LD2 3BWTel: 01982 553 292 | Llandrindod Wells CampusDyffryn Rd, Llandrindod Wells, Powys, LD1 6AWTel: 01597 822 992 |

**‘If we are safe online, we can all enjoy the internet’s abundant resources of information, entertainment, and social connection – while guarding against dangers and risks which can turn our internet experience from good to bad.’**

 **Paul Fletcher, Chief Executive, BCS (British Computing Society)**

Contents:

|  |  |
| --- | --- |
| Development/Monitoring/Review of this Policy | 3 |
| Roles and Responsibilities | 4 |
| Policy Statements | 7 |
| Communications | 14 |
| Dealing with unsuitable/inappropriate activities | 16 |
| Responding to incidents of misuse | 19 |
| Illegal Incidents | 20 |
| Other incidents | 21 |
| School Actions | 22 |
| Appendix | 23 |
| *Section A – Acceptable Use**Section B – Specific Policies**Section C – Support Documents and Links* | *24**30**44* |

### Schedule for Development/Monitoring/Review

5

|  |  |
| --- | --- |
| This online safety policy was approved by the Board of Directors/Governing Body/Governors Sub Committee on: | *Insert date* |
| The implementation of this online safety policy will be monitored by the: | *YCC Online Safety Group* |
| Monitoring will take place at regular intervals: | *Once a year* |
| The Board of Directors/Governing Body/Governors Sub Committee will receive a report on the implementation of the online safety policy generated by the monitoring group (which will include anonymous details of online safety incidents) at regular intervals: | *Summer 2022* |
| The online 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 online safety or incidents that have taken place. The next anticipated review date will be: | *Summer 2022* |
| Should serious online safety incidents take place, the following external persons/agencies should be informed: | *Local Authority Safeguarding Lead*  |

The school will monitor the impact of the policy using:

* Logs of reported incidents
* Internal monitoring data for network activity
* Monitoring of Go4Schools behaviour logs
* Surveys/questionnaires of
	+ students/pupils
	+ parents/carers
	+ staff

6

### Scope of the Policy

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

##

## Roles and Responsibilities

7

The following section outlines the online safety roles and responsibilities of individuals and groups within Ysgol Calon Cymru

**Governors**

Governors are responsible for the approval of the online safety policy and for reviewing the effectiveness of the policy. This will be carried out by the Teaching & Learning/Wellbeing Sub Committee receiving regular information about online safety incidents and monitoring reports. A member of the Governing Body will take on the role of Online Safety Link Governor. The role of the Online Safety Link Governor will include:

* Termly progress meetings with the Ysgol Calon Cymru Online Safety Group
* Attendance at Online Safety Group meetings
* Reporting to relevant Governing Body Sub-Committee meetings.

###

### Headteacher and Senior Leaders

* The Headteacher has a duty of care for ensuring the safety (including online safety) of members of the school community, though the day to day responsibility for online safety will be delegated to the Safeguarding Officers/Online Safety Lead on each campus
* The Headteacher, Safeguarding Officers/Online Safety Lead, Deputy Safeguarding Officers and the Lead on Digital Developments should be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff. (see flow chart on dealing with online safety incidents – included in a later section – “Responding to incidents of misuse” disciplinary procedures).
* The Headteacher is responsible for ensuring that the Safeguarding Officers/Online Safety Lead and other relevant staff receive suitable training to enable them to carry out their online safety roles and to train other colleagues, as relevant.
* The Headteacher and 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 online 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 will receive regular monitoring reports from the Online Safety Lead.

### Online Safety Lead

* leads the Online Safety Group
* takes day to day responsibility for online safety issues and has a leading role in establishing and reviewing the school online safety policies/documents
* ensures that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place.
* provides training and advice for staff
* liaises with the Local Authority
* liaises with school technical staff
* receives reports of online safety incidents and creates a log of incidents to inform future online safety developments.
* meets termly with Online Safety Link Governor to discuss current issues, review incident logs and other relevant information
* attends relevant meetings of Governing Body Sub-Committees
* reports regularly to Senior Leadership Team

**Network Manager**

Those with technical responsibilities are responsible for ensuring:

* that Ysgol Calon Cymru’s technical infrastructure is secure and is not open to misuse or malicious attack
* that Ysgol Calon Cymru meets required online safety technical requirements and any Local Authority online safety policy/guidance that may apply.
* that users may only access the networks and devices through a properly enforced password protection policy
* that filtering is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person.
* that they keep up to date with online safety technical information in order to effectively carry out their online safety role and to inform and update others as relevant
* that the use of any digital technologies is regularly monitored in order that any misuse/attempted misuse can be reported to theOnline Safety Leadand/or Senior Leaders/Headteacher for investigation/action/sanction.
* that monitoring software/systems are implemented and updated as agreed in school policies.

### Teaching and Support Staff

Are responsible for ensuring that:

* they have an up to date awareness of online safety matters and of the current Ysgol Calon Cymruonline safety policy and practices
* they have read, understood and signed the staff acceptable use policy/agreement.
* they report any suspected misuse or problem to the Headteacher/Senior Leader/Online Safety Leadfor investigation/action/sanction
* all digital communications with students/pupils/parents/carers should be on a professional level and only carried out using official school systems
* online safety issues are embedded in all aspects of the curriculum and other activities
* students/pupils understand and follow the Online Safety Policy and acceptable use policies
* students/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 students/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.

**Designated Safeguarding Officers**

Should be trained in online safety issues and be aware of the potential for serious child protection/safeguarding issues to arise from:

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

### Online Safety Group

The Online Safety Group provides a consultative group that has representation from the Ysgol Calon Cymru community, with responsibility for issues regarding online safety and the monitoring the Online Safety Policy including the impact of initiatives. The group will also be responsible for regular reporting to the relevant Governing Body Sub-Committees.

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

* the review/monitoring of the school online safety policy/documents.
* mapping andreviewing the online safety/digital literacy curricular provision – ensuring relevance, breadth and progression
* monitoring network/internet/filtering/incident logs
* consulting stakeholders – including parents/carers and the students/pupils about the online safety provision
* monitoring improvement actions identified through use of the 360 degree safe self-review tool

### Learners:

* are responsible for using Ysgol Calon Cymru digital technology systems in accordance with the student/pupil acceptable use agreement
* have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
* need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
* will be expected to know and understand policies on the use of mobile devices and digital cameras. They should also know and understand policies on the taking/use of images and on online-bullying.
* should understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the Ysgol Calon Cymru online safety policy covers their actions out of school, if related to their membership of the school.

### Parents/carers

Parents/carers play a crucial role in ensuring that their children understand the need to use the internet/mobile devices in an appropriate way. Ysgol Calon Cymru will take every opportunity to help parents understand these issues through appropriate school communications channels and information about national/local online safety campaigns/literature. Parents and carers will be encouraged to support Ysgol Calon Cymru in promoting good online safety practice and to follow guidelines on the appropriate use of:

* digital and video images taken at school events
* access to parents’ sections of the website/school VLE and on-line student/pupil records
* their children’s personal devices inYsgol Calon Cymru (where applicable)

11

## Policy Statements

### Education – Learners

Whilst regulation and technical solutions are very important, their use must be balanced by educating learners to take a responsible approach. The education of learners in online safety/digital literacy is therefore an essential part of Ysgol Calon Cymru’s online safety provision. Children and young people need the help and support of the school to recognise and avoid online safety risks and build their resilience.

Online safety should be a focus in all areas of the curriculum and staff should reinforce online safety messages across the curriculum. The online safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways:

A planned online safety curriculum should be provided as part of ICT and PHSE lessons and should be regularly revisited

* Key online safety messages should be reinforced as part of a planned programme of assemblies and tutorial activities
* Learners should be taught in all lessons to be critically aware of the content they access on-line and be guided to validate the accuracy of information.
* Learners should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
* Learners should be supported in building resilience to radicalisation by providing a safe environment for debating controversial issues and helping them to understand how they can influence and participate in decision-making.
* Learners 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 Ysgol Calon Cymru.
* 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 learners 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 learners 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 online 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 online behaviours. 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.

Ysgol Calon Cymru will therefore seek to provide information and awareness to parents and carers through:

* Letters, newsletters, web site, Learning Platform
* Parents/carers evenings/sessions
* High profile events/campaigns e.g. Safer Internet Day
* Reference to the relevant web sites/publications.

###

### Education – The Wider Community

Ysgol Calon Cymru will provide opportunities for members of the community to gain from our online safety knowledge and experience. This may be offered through the following:

* Providing family learning courses in use of new digital technologies, digital literacy and online safety
* Online safety messages targeted towards grandparents and other relatives as well as parents.
* The Ysgol Calon Cymru website will provide, where appropriate, online safety information for the wider community
* Sharing their online safety expertise/good practice with other local schools
* Supporting community groups e.g. Early Years Settings, Childminders, youth/sports/voluntary groups to enhance their online safety provision*.*

### Education & Training – Staff/Volunteers

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

* A planned programme of formal online safety training will be made available to staff. This will be regularly updated and reinforced. An audit of the online safety training needs of all staff will be carried out regularly.
* All new staff should receive online safety training as part of their induction programme, ensuring that they fully understand the school/academy online safety policy and acceptable use agreements.
* It is expected that some staff will identify online safety as a training need within the line management process.
* The Online Safety Lead (or other nominated person) will receive regular updates through attendance at external training events and by reviewing guidance documents released by relevant organisations.
* This online safety policy and its updates will be presented to and discussed by staff in staff/team meetings/training sessions.
* The Online Safety Lead (or other nominated person) will provide advice/guidance/training to individuals as required.

### Training – Governors

Governors should take part in online safety training/awareness sessions, with particular importance for those who are members of any group involved in online 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.
* Participation in Ysgol Calon Cymru sessions for staff or parents.

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

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

Ysgol Calon Cymru 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 school IT Network Manager who will keep an up to date record of users and their usernames.Users are responsible for the security of their username and password.
* Governors, staff and learners will have access to a username and password for the National HWB network where nominated staff have limited administration rights as digital champions.
* The “administrator” passwords for the school systems, used by the Network Manager must also be available to the Headteacher or Senior Leader responsible for Digital Developments and kept securely (e.g. school safe)
* the school IT Network Manager 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
* 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.
* Internet filtering/monitoring should ensure that children are safe from terrorist and extremist material when accessing the internet.
* Ysgol Calon Cymruhas provided enhanced/differentiated user-level filtering*.*
* Ysgol Calon Cymrutechnical 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.
* users need to report any actual/potential technical incident/security breach to the IT Network Manager; Online Safety Lead or any other senior member of staff.
* 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 devices are protected by up to date virus software.
* An agreed policy is in place for the provision of temporary access of “guests” (e.g. 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 that allows staff to/forbids staff from downloading executable files and installing programmes on school devices.
* An agreed policy is in place regarding the use of removable media (e.g. 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*.*

### Mobile Technologies (including BYOD/BYOT)

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

All users should understand that the primary purpose of the use mobile/personal devices in a school context is educational. The mobile technologies policy should be consistent with and inter-related to other relevant school polices including but not limited to the safeguarding policy, behaviour policy, bullying policy, acceptable use policy, and policies around theft or malicious damage. Teaching about the safe and appropriate use of mobile technologies should be an integral part of the school’s online safety education programme.

* The school acceptable use agreements for staff, pupils/students and parents/carers will consider the use of mobile technologies
* The school allows:

|  |  |  |
| --- | --- | --- |
|  | School Devices | Personal Devices |
|  | **School owned for single user** | **School owned for multiple users** | **Authorised device[[1]](#footnote-1)** | **Student owned** | **Staff owned** | **Visitor owned** |
| Allowed in school | Yes | Yes | Yes | Yes | Yes | Yes |
| Full network access | Yes | Yes | Yes | No | No | No |
| Internet only |  |  |  |  |  |  |
| No network access |  |  |  |  |  |  |

Aspects that the school may wish to consider and be included in their online safety policy, mobile technologies policy or acceptable use agreements:

#### School owned/provided devices:

* *Who they will be allocated to*
* Where, when and how their use is allowed – times/places/in school/out of school
* If personal use is allowed
* Levels of access to networks/internet (as above)
* Management of devices/installation of apps/changing of settings/monitoring
* Network/broadband capacity
* Technical support
* Filtering of devices
* Access to cloud services
* Data Protection
* Taking/storage/use of images
* Exit processes – what happens to devices/software/apps/stored data if user leaves the school
* Liability for damage
* Staff training

#### Personal devices:

* Which users are allowed to use personal mobile devices in school (staff/pupils/students/visitors)
* Restrictions on where, when and how they may be used in school
* Storage
* Whether staff will be allowed to use personal devices for school business
* Levels of access to networks/internet (as above)
* Network/broadband capacity
* Technical support (this may be a clear statement that no technical support is available)
* Filtering of the internet connection to these devices
* Data Protection
* The right to take, examine and search users devices in the case of misuse (England only) – N.B. this must also be included in the Behaviour Policy.
* Taking/storage/use of images
* Liability for loss/damage or malfunction following access to the network (likely to be a disclaimer about school responsibility).
* Identification/labelling of personal devices
* How visitors will be informed about school requirements
* How education about the safe and responsible use of mobile devices is included in the school online safety education programmes.

### Use of digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and learners instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents/carers and learners need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for online-bullying 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 learners about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.
* Written permission from parents or carers will be obtained before photographs of learners are published on the school website/social media/local press.
* 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/academy events for their own personal use (as such use in 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 learners in the digital/video images.
* Staff and volunteers are allowed to take digital/video images to support educational aims, but must follow school/academy policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school/academy equipment; the personal equipment of staff should not be used for such purposes.
* Care should be taken when taking digital/video images that learners are appropriately dressed and are not participating in activities that might bring the individuals or the school/academy into disrepute.
* Learners must not take, use, share, publish or distribute images of others without their permission
* Photographs published on the website, or elsewhere that include learners will be selected carefully and will comply with good practice guidance on the use of such images.
* Learners full names will not be used anywhere on a website or blog, particularly in association with photographs.
* Learners work can only be published with the permission of the learners and parents or carers.

### Data Protection

Personal data will be recorded, processed, transferred and made available according to the current data protection legislation.

#### Ysgol Calon Cymru will ensure that:

* it has a Data Protection Policy. (see appendix for template policy)
* it implements the data protection principles and is able to demonstrate that it does so through use of policies, notices and records.
* it has paid the appropriate fee Information Commissioner’s Office (ICO) and included details of the Data Protection Officer (DPO).
* it has appointed an appropriate Data Protection Officer (DPO) who has a high level of understanding of data protection law and is free from any conflict of interest.
* it has an ‘information asset register’ in place and knows exactly what personal data it holds, where this data is held, why and which member of staff has responsibility for managing it
* the information asset register records the lawful basis for processing personal data (including, where relevant, how consent was obtained and refreshed). Where special category data is processed, an additional lawful basis will have also been recorded
* it will hold only 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. The school should develop and implement a ‘retention policy” to ensure there are clear and understood policies and routines for the deletion and disposal of data to support this. personal data held must be accurate and up to date where this is necessary for the purpose it is processed for. Have systems in place to identify inaccuracies, such as asking parents to check emergency contact details at suitable intervals
* it provides staff, parents, volunteers, teenagers and older children with information about how the school/academy looks after their data and what their rights are in a clear Privacy Notice (see Privacy Notice section in the appendix)
* procedures must be in place to deal with the individual rights of the data subject, e.g. one of the 8 data subject rights applicable is that of Subject Access which enables an individual to see to have a copy of the personal data held about them (subject to certain exceptions which may apply).
* data Protection Impact Assessments (DPIA) are carried out where necessary. For example, to ensure protection of personal data when accessed using any remote access solutions, or entering into a relationship with a new supplier (this may also require ensuring that data processing clauses are included in the supply contract or as an addendum)
* it has undertaken appropriate due diligence and has required data processing clauses in contracts in place with any data processors where personal data is processed.
* it understands how to share data lawfully and safely with other relevant data controllers.
* it [reports any relevant breaches to the Information Commissioner](https://ico.org.uk/for-organisations/report-a-breach/) within 72hrs of becoming aware of the breach in accordance with UK data protection law. It also reports relevant breaches to the individuals affected as required by law. In order to do this, it has a policy for reporting, logging, managing, investigating and learning from information risk incidents.
* If a maintained school/academy, it must have a Freedom of Information Policy which sets out how it will deal with FOI requests.
* all staff receive data protection training at induction and appropriate refresher training thereafter. Staff undertaking particular data protection functions, such as handling requests under the individual’s rights, will receive training appropriate for their function as well as the core training provided to all staff.

#### When personal data is stored on any mobile device or removable media the:

* data must be encrypted and password protected.
* device must be password protected.
* device must be protected by up to date virus and malware checking software

16

* data must be securely deleted from the device, in line with school/academy policy (below) once it has been transferred or its use is complete.

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
* can recognise a possible breach, understand the need for urgency and know who to report it to within the school
* can help data subjects understands their rights and know how to handle a request whether verbal or written. Know who to pass it to in the school
* where personal data is stored or transferred on mobile or other devices (including USBs) these must be encrypted and password protected.
* will not transfer any school/academy personal data to personal devices except as in line with school policy
* access personal data sources and records 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

## Communications

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

|  |  |  |
| --- | --- | --- |
|  | **Staff & Other Adults** | **Learners** |
| **Communication****Technologies** | Allowed | Allowed at certain times | Allowed for selected staff | Not Allowed | Allowed | Allowed at certain times | Allowed with staff permission | Not Allowed |
| Mobile Phones may be brought to school | **x** |  |  |  | **x** |  |  |  |
| Use of Mobile phones in lessons |  | **x** |  |  |  |  | **x** |  |
| Use of mobile phones in social time |  | **x** |  |  |  |  |  | **x** |
| Taking photos on mobile phones / cameras |  |  |  | **x** |  |  |  | **x** |
| Use of other mobile devices e.g. tablets, gaming devices. |  | **x** |  |  |  |  | **x** |  |
| Use of personal email addresses in school, or on school network |  |  |  | **x** |  |  |  | **x** |
| Use of school email for personal emails |  |  |  | **x** |  |  |  | **x** |
| Use of messaging apps |  | **x** |  |  |  |  |  | **x** |
| Use of social media |  |  | **x** |  |  |  |  | **x** |
| Use of Blogs |  |  |  | **x** |  |  |  |  |

Staff should follow the staff policy: ‘CYNGOR SIR POWYS COUNTY COUNCIL Use of Social Media and E-safety policy for staff working in schools’

When using communication technologies, Ysgol Calon Cymru considers the following as good practice:

* The official Ysgol Calon Cymru email service is situated on the National HWB platform and may be regarded as safe and secure and is monitored.Users should be aware that email communications are monitored. Staff and learners should therefore use only the HWB email service to communicate with others when in school, or on school systems (e.g. 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 learners or parents/carers (email, social media, chat, blogs, VLE etc) must be professional in tone and content. These communications may only take place on the official school system i.e through the HWB Network. Personal email addresses, text messaging or social media must not be used for these communications.
* Learners should be taught about online 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 Ysgol Calon Cymru website and only official email addresses should be used to identify members of staff.

### Social Media - Protecting Professional Identity

All schools and local authorities have a duty of care to provide a safe learning environment for learners 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, engage in online bullying, 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.

Ysgol Calon Cymru provides the following measures to ensure reasonable steps are in place to minimise risk of harm to learners, staff and the school through:

* Ensuring that personal information is not published
* Training is provided including: 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

Ysgol Calon Cymru should ensure that:

* No reference should be made in social media to learners, parents/carers or school staff by name.
* 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 schoolor local authority.
* Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

#### When official school social media accounts are established there should be:

* A process for approval by senior leaders
* Clear processes for the administration and monitoring of these accounts – involving at least two members of staff
* A code of behaviour for users of the accounts, including
* Systems for reporting and dealing with abuse and misuse
* Understanding of how incidents may be dealt with under school disciplinary procedures

#### Personal Use:

* Personal communications are those made via a personal social media accounts. In all cases, where a personal account is used which associates itself with Ysgol Calon Cymru or impacts on Ysgol Calon Cymru, it must be made clear that the member of staff is not communicating on behalf of Ysgol Calon Cymru with an appropriate disclaimer. Such personal communications are within the scope of this policy
* Personal communications which do not refer to or impact upon the school are outside the scope of this policy
* Where excessive personal use of social media in school is suspected, and considered to be interfering with relevant duties, disciplinary action may be taken
* The school permits reasonable and appropriate access to private social media sites

#### Monitoring of Public Social Media:

* As part of active social media engagement, it is considered good practice to pro-actively monitor the Internet for public postings about the school
* The school should effectively respond to social media comments made by others according to a defined policy or process

Ysgol Calon Cymru’s use of social media for professional purposes will be checked regularly by the Digital Lead and Online Safety Group to ensure compliance with the school policies.

##

## Dealing with unsuitable/inappropriate activities

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

Ysgol Calon Cymru 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/or outside the school when using school equipment or systems. Ysgol Calon Cymru policy restricts usage as follows:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| User Actions18 | 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 |
| Promotion of extremism or terrorism |  |  |  |  | X |
| Any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute |  |  |  | X |  |
| Activities that might be classed as cyber-crime under the Computer Misuse Act:* Gaining unauthorised access to school networks, data and files, through the use of computers/devices
* Creating or propagating computer viruses or other harmful files
* Revealing or publicising confidential or proprietary information (e.g. financial / personal information, databases, computer / network access codes and passwords)
* Disable/Impair/Disrupt network functionality through the use of computers/devices
* Using penetration testing equipment (without relevant permission)
 |  |  |  |  | X |
| Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school/academy |  |  |  | X |  |
| Revealing or publicising confidential or proprietary information (e.g. financial/personal information, databases, computer/network access codes and passwords) |  |  |  | X |  |
| Unfair usage (downloading/uploading large files that hinders others in their use of the internet) |  |  |  | X |  |
| Using school systems to run a private business |  |  |  | X |  |
| Infringing copyright |  |  |  | X |  |
| On-line gaming (educational) |  | X |  |  |  |
| On-line gaming (non-educational) |  |  |  | X |  |
| On-line gambling |  |  |  | X |  |
| On-line shopping/commerce |  |  |  | X |  |
| File sharing |  | X |  |  |  |
| Use of social media  |  |  | X |  |  |
| Use of messaging apps |  |  |  | X |  |
| Use of video broadcasting e.g. Youtube19 |  | X |  |  |  |

##

## 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 Ysgol Calon Cymru community will be responsible users of digital technologies, who understand and follow school policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse.

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

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

It is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the school community are aware that incidents have been dealt with.

Each incident will be investigated fully. Appropriate sanctions will be issued depending on the severity and context of the incident.

Possible sanctions may include:

**For Pupils**

Refer to class teacher/tutor

Refer to Head of Department/Year/other

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 e.g. detention/exclusion

**For Staff**

Refer to line manager

Refer to Headteacher Principal

Refer to Local Authority/HR

Refer to Police.

Refer to Technical Support Staff for action re filtering etc.

Warning.

Suspension.

Disciplinary action.

**Appendix**

**Appendices – Section A - Acceptable Use Agreement**

• A1 Student / Pupil Acceptable Use Agreement

• A2 Staff and Volunteers Acceptable Use Agreement

**Appendices – Section B – Specific Policies**

• B1 School Technical Security Policy

• B2 School Personal Data Guidance and Advice

**Appendices – Section C – Support documents and links**

• C1 Record of reviewing sites (for internet misuse)

• C2 School Reporting Log template

• C3 Summary of Legislation

• C4 Links to other organisations and documents

• C6 Glossary of terms

## A1 - Student/Pupil Acceptable Use Agreement

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 access to these digital technologies.

### 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 will have good access to digital technologies to enhance their learning and will, in return, expect learner*s* to agree to be responsible users.

### Acceptable Use Agreement

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

### For my own personal safety:

* I understand that Ysgol Calon Cymru will monitor my use of the 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 Ysgol Calon Cymru 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 Ysgol Calon Cymru systems or devices for on-line gaming, on-line gambling, internet shopping, file sharing, or video broadcasting (e.g. YouTube), unless I have permission of a member of staff to do so.

25

### 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 Ysgol Calon Cymru:

* I will only use my own personal devices (mobile phones/USB devices etc.) in school if I have permission). I understand that, if I do use my own devices in Ysgol Calon Cymru 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 understand that I am not permitted to use social media sites during school hours.

### 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 Ysgol Calon Cymru 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 online-bullying, use of images or personal information).
* I understand that if I fail to comply with this acceptable use agreement, I may be subject to disciplinary action. This could 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.**

###

### Student/Pupil Acceptable Use Agreement Form

This form relates to the student/pupil acceptable use agreement; to which it is attached.

Please complete the sections below 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.

I have read and understand the above and agree to follow these guidelines when:

* I use Ysgol Calon Cymru systems and devices (both in and out of school)
* I use my own devices in Ysgol Calon Cymru (when allowed) e.g. mobile phones, gaming devices USB devices, cameras etc.
* I use my own equipment out of Ysgol Calon Cymru in a way that is related to me being a member of this school e.g. communicating with other members of the school, accessing school email, VLE, website etc.

Name of Student/Pupil:

Group/Class:

Signed:

Date:

### Parent/Carer Countersignature

Name of Parent/Carer

Signed:

Date:

## A2 - Staff (and Volunteer) Acceptable Use Policy Agreement

### School Policy

New technologies have become integral to the lives of children and young people in today’s society, both within schools/academies 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 access to the internet and digital technologies 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 Ysgol Calon Cymru 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 technology in their everyday work.

The school will try to ensure that staff and volunteers will have good access to digital technology to enhance their work, to enhance learning opportunities for 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 systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems and other users. I recognise the value of the use of digital technology for enhancing learning and will ensure that learners receive opportunities to gain from the use of digital technology. I will, where possible, educate the young people in my care in the safe use of digital technology and embed online safety in my work with young people.

### For my professional and personal safety:

* I understand that Ysgol Calon Cymru will monitor my use of the school digital technology and communications systems.
* I understand that the rules set out in this agreement also apply to use of these technologies (e.g. 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 digital technology 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.
* 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.

28

### I will be professional in my communications and actions when using Ysgol Calon Cymru 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 (e.g. 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 social networking sites in school in accordance with the school’s policies.
* I will only communicate with learners and parents/carers using official school systems. Any such communication will be professional in tone and manner.
* 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 Ysgol Calon Cymru:

* When I use my mobile devices in school, I will follow the rules set out in this agreement, in the same way as if I was using Ysgol Calon Cymru equipment. I will also follow any additional rules set by Ysgol Calon Cymru 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 use personal email addresses on the school/academy ICT systems.
* 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/academy policies.
* I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, terrorist or extremist 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/academy policies.
* I will not disable or cause any damage to school/academy 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/Academy/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 documents containing personal 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/academy 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 Ysgol Calon Cymru:

* I understand that this acceptable use policy applies not only to my work and use of Ysgol Calon Cymru digital technology equipment in school, but also applies to my use of Ysgol Calon Cymru 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/academy
* I understand that if I fail to comply with this acceptable use agreement, I could be subject to disciplinary action. This could include 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 digital technology 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:

## B1 - School Technical Security Policy Template (including filtering and passwords)

### 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 the local authority (Powys CC); the external ICT Provider (Calibre Solutions) in conjunction with the school Network Manager.

### Technical Security

### Policy statements

Ysgol Calon Cymru will be responsible for ensuring that their 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 receive guidance and training and will be effective in carrying out their responsibilities:

* **Ysgol Calon Cymru 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/academy 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 and will be reviewed, at least annually, by the network manager and digital lead for Ysgol Calon Cymru.**
* **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*.***
* The school Network Manager 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
* Calibre Solutions and the school network manage 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.
* remote management tools are used by staff to control workstations and view users activity
* users are to report any actual/potential technical incident to the network manager via the school ICT Helpdesk ticketing system (users are discouraged from emailing the school network manager on technical issues).
* the provision of temporary access of “guests”, (e.g. trainee teachers, supply teachers, visitors) onto the school system is provided by the school network manager.
* the downloading of executable files and the installation of programmes on school/academy devices by users is enabled by the Network Manager only
* an agreed policy is in place (see Appendix A2 – “Staff/Volunteer Acceptable Use Policy Agreement”) regarding the extent of personal use that users (staff/learners/community users) and their family members are allowed on school devices that may be used out of school.
* an agreed policy is in place (see Appendix A2 – “Staff/Volunteer Acceptable Use Policy Agreement”) regarding the use of removable media (e.g. 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 learning platform.

###

### Policy Statements:

These statements apply to all users.

* All school networks and systems will be protected by secure passwords.
* All users 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 and will be reviewed, at least annually, by the online safety group (or other group).
* All users 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.
* Passwords must not be shared with anyone.
* All users will be provided with a username and password to access the school system. The school Network Manager who will keep an up to date record of users and their usernames.

### Password requirements:

* Passwords should be long. Good practice highlights that passwords over 12 characters in length are considerably more difficult to compromise than shorter passwords. Passwords generated by using a combination of unconnected words that are over 16 characters long are extremely difficult to crack. Password length trumps any other special requirements such as uppercase/lowercase letters, number and special characters. Passwords should be easy to remember, but difficult to guess or crack.
* 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/academy
* Passwords must not include names or any other personal information about the user that might be known by others
* Passwords must be changed on first login to the system

### Learner passwords:

* Records of learner usernames and passwords for foundation phase students/pupils can be kept in an electronic or paper-based form, but they must be securely kept when not required by the user. Password complexity in foundation phase should be reduced (for example 6-character maximum) and should not include special characters. Where external systems have different password requirements the use of random words or sentences should be encouraged.
* Users will be required to change their password if it is compromised.
* Students/pupils will be taught the importance of password security, this should include how passwords are compromised, and why these password rules are important.

###

### Notes for technical staff/teams

* Each administrator should have an individual administrator account, as well as their own user account with access levels set at an appropriate level. Consideration should also be given to using two factor authentication for such accounts.
* An administrator account password for the school/academy systems should also be kept in a secure place This account and password should only be used to recover or revoke access. Other administrator accounts should not have the ability to delete this account.
* Any digitally stored administrator passwords should be hashed using a suitable algorithm for storing passwords (e.g. Bcrypt or Scrypt). Message Digest algorithms such as MD5, SHA1, SHA256 etc. should not be used.
* It is good practice that where passwords are used there is a user-controlled password reset process to enable independent, but secure re-entry to the system. This ensures that only the owner has knowledge of the password.
* Where user-controlled reset is not possible, passwords for new users, and replacement passwords for existing users will be allocated by the Network Manager; Digital Lead and/or ICT teaching staff from each campus. Users are directed to change password the next time they log in, after being provided with a temporary one.
* Where automatically generated passwords are not possible, then a good password generator should be used by by the Network Manager; Digital Lead and/or ICT teaching staff to provide the user with their initial password. There should be a process for the secure transmission of this password to limit knowledge to the password creator and the user. The password should be temporary and the user should be forced to change their password on the first login*.*
* Requests for password changes should be authenticatedby the Network Manager; Digital Lead and/or ICT teaching staff *to* ensure that the new password can only be passed to the genuine user.
* Suitable arrangements should be in place to provide visitors with appropriate access to systems which expires after use.
* In good practice, the account is “locked out” following six successive incorrect log-on attempts.
* Passwords shall not be displayed on screen, and shall be securely hashed when stored (use of one-way encryption).

###

### Training/Awareness:

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

* at induction
* through the school online safety policy and password security policy
* through the acceptable use agreement

#### Students/pupils will be made aware of the school password policy:

* in ICT lessons
* through the acceptable use agreement

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

The Network Manager will ensure that full records are kept of:

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

### Filtering

36

#### 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 online 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 the Network Manager. 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 – Digital Lead
* be reported to the Online Safety Group every term in the form of an audit of the change control logs

All users have a responsibility to report immediately to the Network Manager 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 the 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. 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.

* Ysgol Calon Cymru maintains and supports the managed filtering service provided by the Internet Service Provider. The school is supported in this process by the Local Authority and Calibre Solutions.
* In the event of the technical staff needing to switch off the filtering for any reason, or for any user, this must be logged and carried out by a process that is agreed by the Digital Lead
* Mobile devices that access the school/academy internet connection (whether school/academy 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 Network Manager or Digital Lead. If the request is agreed, this action will be recorded and logs of such actions shall be reviewed regularly by the Online Safety Group.

### Education/Training/Awareness

Pupils/students will be made aware of the importance of filtering systems through the online 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
* induction training
* staff meetings, briefings, Inset.

Parents will be informed of the school’s filtering policy through the acceptable use agreement and through online safety awareness sessions/newsletter etc.

### Changes to the Filtering System

In this section the school should provide a detailed explanation of:

* users may request changes to the filtering system to the Network Manager and/or Digital Lead.
* changes to the filtering system may need to be discussed with the school head and/or governing body, depending on the context of the change.
* requests may be allowed or denied according to each individual case. Alternative solutions to the original request may be suggested by the network manager and/or Digital Lead.
* checks and balances may be undertaken retrospectively through inspection of records/audit of logs.

Users who gain access to, or have knowledge of others being able to access, sites which they feel should be filtered (or unfiltered) should report this in the first instance to the Network Manager, who will decide whether to make school level changes (as above).

### 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 online safety policy and the acceptable use agreement.

### Audit/Reporting

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

* the Digital Lead
* Online Safety Group
* Online Safety Governor/Governors committee
* External Filtering provider/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.

### Further Guidance

35

Schools in England and Wales are required *“to ensure children are safe from terrorist and extremist material when accessing the internet in school, including by establishing appropriate levels of filtering"* ([Revised Prevent Duty Guidance: for England and Wales, 2015](https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/445977/3799_Revised_Prevent_Duty_Guidance__England_Wales_V2-Interactive.pdf)).

The Department for Education ‘[Keeping Children Safe in Education’](https://www.gov.uk/government/publications/keeping-children-safe-in-education--2)requires schools to: *“ensure appropriate filters and appropriate monitoring systems are in place. Children should not be able to access harmful or inappropriate material from the school or colleges IT system”* however, schools will need to *“be careful that “over blocking” does not lead to unreasonable restrictions as to what children can be taught with regards to online teaching and safeguarding.”*

In response UKSIC produced guidance on – information on “[Appropriate Filtering](http://www.saferinternet.org.uk/advice-and-resources/teachers-and-professionals/appropriate-filtering-for-education-settings)”

## B2 - School Personal Data Advice and Guidance

### Data Protection Law – A Legislative Context

With effect from 25th May 2018, the data protection arrangements for the UK changed following the implementation of the European Union General Data Protection Regulation (GDPR). This represented a significant shift in legislation and in conjunction with the Data Protection Act 2018 replaced the Data Protection Act 1998.

GDPR - As a European Regulation, the GDPR has direct effect in UK law and automatically applies in the UK until we leave the EU (or until the end of any agreed transition period, if we leave with a deal). After this date, it will form part of UK law under the European Union (Withdrawal) Act 2018, with some technical changes to make it work effectively in a UK context.

Data Protection Act 2018 – this Act sits alongside the GDPR, and tailors how the GDPR applies in the UK and provides the UK-specific details such as; how to handle education and safeguarding information.

No Deal Brexit -The Information Commissioner advises that in the event of a no- deal Brexit it is anticipated that the Government of the day will pass legislation to incorporate GDPR into UK law alongside the DPA 2018. Unless your school/academy receives personal data from contacts in the EU there will be little change save to update references to the effective legislation in privacy notices etc.

In this document the term “Data Protection Law” refers to the legislation applicable to data protection and privacy as applicable in the UK from time to time.

### Does the Data Protection Law apply to schools?

In short, yes. Any natural or legal person, public authority, agency or other body which processes personal data is considered a ‘data controller’.

A school/academy is, for the purposes of the Data Protection Law, a “public body” and further processes the **personal data** of numerous **data subjects** on a daily basis.

Personal data is information that relates to an identified or identifiable living individual (a data subject).

Guidance for schools/academies is available on the [Information Commissioner’s Office](https://ico.org.uk/for-organisations/education/) (ICO) website including information about the Data Protection Law.

The ICO’s powers are wide ranging in the event of non-compliance and schools/academies must be aware of the huge impact that a fine or investigation will have on finances and also in the wider community for example in terms of trust.

The Data Protection Law sets out that a data controller must ensure that personal data shall be:

a) processed lawfully, fairly and in a transparent manner in relation to data subjects;

b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;

c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;

e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the Data Protection Law in order to safeguard the rights and freedoms of data subjects; and

f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

These principles of the Data Protection Law drive the need for the school/academy to put in place appropriate **privacy notices** (to give a data subject information about the personal data processing activities, **legal basis of processing** and **data subject rights**) and policies (such as for reporting a breach, managing a data subject access request, training, retention etc.) to demonstrate compliance.

### Data Mapping to identify personal data, data subjects and processing activities

Ysgol Calon Cymru and its employees will collect and/ or process a wide range of information concerning numerous data subjects and some of this information will include personal data. Further, the school/academy may need to share some personal data with third parties. To be able to demonstrate and plan compliance and it is important that the school/academy has a **data map** of these activities; it can then make sure that the correct privacy notices are provided, put in place **security measures** to keep the personal data secure and other steps to avoid **breach** and also put in place data processing agreements with the third parties.

The data map should identify what personal data held in digital format or on paper records in a school/ academy, where it is stored, why it is processed and how long it is retained.

In a typical data map for a school the data subjects and personal data will include, but is not limited to:

* Parents, legal guardians, governors – and personal data of names, addresses, contact details
* Learners - curricular / academic data e.g. class lists, learner progress records, reports, references, contact details, health and SEN reports
* Staff and contractors - professional records e.g. employment history, taxation and national insurance records, appraisal records and references, health records

### Some types of personal data are designated as ‘special category’ being personal data;

“revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person’s sex life or sexual orientation”

This should be identified separately and to lawfully process special category data, you must identify both a [lawful basis](#1v1yuxt) and a [separate condition for processing special category data](https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/special-category-data/). You should decide and document this before you start processing the data.

The school/academy will need to identify appropriate lawful process criteria for each type of personal data and if this is not possible such activities should be discontinued. The lawful processing criteria can be summarised as:

(a) Consent: the data subject has given clear consent for you to process their personal data for a specific purpose (see below for further guidance)

(b) Contract: the processing is necessary for a contract you have with the data subject

(c) Legal obligation:  the processing is necessary for you to comply with the law (not including contractual obligations).

(d) Vital interests:  the processing is necessary to protect someone’s life.

(e) Public task:  the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.

(f) Legitimate interests:  the processing is necessary for your legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual’s personal data which overrides those legitimate interests. (This cannot apply if you are a public authority processing data to perform your official tasks) Please also be aware that these criteria must be supported by a written legitimate interest assessment.

No single basis is ’better’ or more important than the others – which basis is most appropriate to use will depend on your purpose and relationship with the data subject.

Several of the lawful purpose criteria may relate to a particular specified purpose – a legal obligation, a contract with the individual, protecting someone’s vital interests, or performing your public tasks. If you are processing for these purposes then the appropriate lawful basis may well be obvious, so it is helpful to consider these first.

As a public authority, and if you can demonstrate that the processing is to perform your tasks as set down in UK law, then you are able to use the public task basis. If not, you may still be able to consider consent or legitimate interests in some cases, depending on the nature of the processing and your relationship with the data subject. There is no absolute ban on public authorities using consent or legitimate interests as their lawful basis, but the Data Protection law does restrict public authorities’ use of these two criteria.

The majority of processing of personal data conducted by public authorities will fall within Article 6(1)(e) GDPR, that *“processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller”* however careful consideration must be given to any processing, especially in more novel areas. As you can see, consent is just one of several possible lawful processing criteria.

Consent has changed as a result of the GDPR and is now defined as: “in relation to the processing of personal data relating to an individual, means a freely given, specific, informed and unambiguous indication of the individual’s wishes by which the individual, by a statement or by a clear affirmative action, signifies agreement to the processing of the personal data”

This means that where a school/academy is relying on consent as the basis for processing personal data that consent has to be clear, meaning that pre-ticked boxes, opt-out or implied consent are no longer suitable. The GDPR does not specify an age of consent for general processing but schools/academies should consider the capacity of pupils to freely give their informed consent.

The Information Commissioner’s Office (ICO) gives clear advice on when it’s appropriate to [use consent](https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/consent/) as a lawful base. It states:

“Consent is appropriate if you can offer people real choice and control over how you use their data and want to build their trust and engagement. But if you cannot offer a genuine choice, consent is not appropriate. If you would still process the personal data without consent, asking for consent is misleading and inherently unfair.”

You should only use consent if none of the other lawful bases is appropriate. If you do so, you must be able to cope with people saying no (and/or changing their minds), so it’s important that you only use consent for optional extras, rather than for core information the school requires in order to function. Examples;

* + consent would be appropriate for considering whether a child's photo could be published in any way.
	+ if your school or academy requires learner details to be stored in an MIS, it would not be appropriate to rely on consent if the learner cannot opt out of this. In this case, you could apply the public task lawful base.

### Content of Privacy Notices

Privacy Notices are a key compliance requirement as they ensure that each data subject is aware of the following points when data is collected/ processed by a data controller:

* Who the controller of the personal data is
* What personal data is being processed and the lawful purpose of this processing
* where and how the personal data was sourced
* to whom the personal data may be disclosed
* how long the personal data may be retained
* data subject’s rights and how to exercise them or make a complaint

In order to comply with the fair processing requirements in data protection law, the school/academy will inform parents/carers of all learners of the data they collect, process and hold on the learners, the purposes for which the data is held and the third parties (e.g. LA etc.) to whom it may be passed. This privacy notice will be passed to parents/carers for example in the prospectus, newsletters, reports or a specific letter / communication or you could publish it on your website and keep it updated there. Parents/carers of young people who are new to the school/academy will be provided with the privacy notice through an appropriate mechanism.

In some circumstances you may also require privacy notices for children / learners as data subjects as children have the same rights as adults over their personal data. These include the rights to access their personal data; request rectification; object to processing and have their personal data erased. The policies that explain this should be clear and age appropriate.

### Data subject’s right of access

Data subjects have a number of rights in connection with their personal data. They have the right:

* to be informed – Privacy Notices
* of access – Subject Access Requests
* to rectification – correcting errors
* to erasure – deletion of data when there is no compelling reason to keep it
* to restrict processing – blocking or suppression of processing
* to portability – unlikely to be used in a school/academy context
* to object – objection based on grounds pertaining to their situation
* related to automated decision making, including profiling

Several of these could impact schools and academies, such as the right of access. You need to put procedures in place to deal with [Subject Access Requests](https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-of-access/). These are written or verbal requests to see all or a part of the personal data held by the Controller in connection with the data subject. Controllers normally have 1 calendar month to provide the information, unless the case is unusually complex in which case an extension can be obtained.

A school must not disclose personal data even if requested in a Subject Access Request;

* if doing so would cause serious harm to the individual
* child abuse data
* adoption records
* statements of special educational needs

Your school or academy must provide the information free of charge. However, if the request is clearly unfounded or excessive – and especially if this is a repeat request – you may charge a reasonable fee.

### Breaches and how to manage a breach

Recent publicity about data breaches suffered by organisations and individuals continues to make the area of personal data protection a current and high profile issue for schools, academies and other organisations. It is important that the school/academy has a clear and well understood personal data handling policy in order to minimise the risk of personal data breaches.

A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes. It also means that a breach is more than just about losing personal data.

A breach may arise from a theft, a deliberate attack on your systems, the unauthorised or malicious use of personal data by a member of staff, accidental loss, or equipment failure. In addition:

* no school or individual would want to be the cause of a data breach, particularly as the impact of data loss on individuals can be severe, put individuals at risk and affect personal, professional or organisational reputation
* schools are “data rich” and the introduction of electronic storage and transmission of data has created additional potential for the loss of data
* the school will want to avoid the criticism and negative publicity that could be generated by anypersonal data breach

Schools have always held personal data on the learners in their care, and increasingly this data is held digitally and accessible not just in school but also from remote locations. It is important to stress that the Data Protection Laws apply to all forms of personal data, regardless of whether it is held on paper or in electronic format. However, as it is part of an overall online safety policy template, this document will place particular emphasis on data which is held or transferred digitally.

Schools will need to carefully review their policy, in the light of pertinent Local Authority regulations and guidance and changes in legislation.

All significant [data protection incidents must be reported](https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/personal-data-breaches/) through the DPO to the Information Commissioner’s Office based upon the local incident handling policy and communication plan. The new laws require that this notification should take place within 72 hours of the breach being detected, where feasible.

If you experience a personal data breach you need to consider whether this poses a risk to people. You need to consider the likelihood and severity of any risk to people’s rights and freedoms, following the breach. When you’ve made this assessment, if it’s likely there will be a risk then you must notify the ICO; if it’s unlikely then you don’t have to report it. You do not need to report every breach to the ICO.

The school/academy should have a policy for reporting, logging, managing and recovering from information risk incidents, which establishes a:

* “responsible person” for each incident
* communications plan, including escalation procedure
* plan of action for rapid resolution
* plan of action of non-recurrence and further awareness raising

### Privacy by Design and Data Protection Impact Assessments (DPIA)

Data Protection Impact Assessments (DPIA) identify and address privacy risks early on in any project so that you can mitigate them before the project goes live.

DPIAs should be carried out by Data Managers (where relevant) under the support and guidance of the DPO. Ideally you should conduct a DPIA before processing activity starts. However, some may need to be retrospective in the early stages of compliance activity.

The risk assessment will involve:

* recognising the risks that are present
* judging the level of the risks (both the likelihood and consequences)
* prioritising the risks.

According to the ICO a DPIA should contain:

* a description of the processing operations and the purpose
* an assessment of the necessity and proportionality of the processing in relation to the purpose
* an assessment of the risks to individuals
* the measures in place to address risk, including security and to demonstrate that you comply.

Or more simply and fully:

* who did you talk to about this?
* what is going to happen with the data and how – collection, storage, usage, disposal
* how much personal data will be handled (number of subjects)
* why you need use personal data in this way
* what personal data (including if it’s in a ‘special category’) are you using
* at what points could the data become vulnerable to a breach (loss, stolen, malicious)
* what the risks are to the rights of the individuals if the data was breached
* what are you going to do in order to reduce the risks of data loss and prove you are compliant with the law.

DPIA is an ongoing process and should be re-visited at least annually to verify that nothing has changed since the processing activity started.

### Secure storage of and access to data

The school should ensure that 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.

[Good practice](https://www.ncsc.gov.uk/guidance/password-guidance-simplifying-your-approach) suggests that all users will use strong passwords made up from a combination of simpler words. User passwords must never be shared.

Personal data may only be accessed on machines that are securely protected. Any device that can be used to access personal 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 should only be stored on school equipment. Private equipment (i.e. owned by the users) must not be used for the storage of school/academy 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
* The device must offer approved virus and malware checking software
* The data must be securely deleted from the device, in line with school/academy policy once it has been transferred or its use is complete.

The school will need to set its own policy as to whether data storage on removal media is allowed, even if encrypted. Some organisations do not allow storage of personal data on removable devices.

The school should have a clear policy and procedures for the automatic backing up, accessing and restoring of all data held on school/academy systems, including off-site backups.

The school should have clear policy and procedures for the use of “Cloud Based Storage Systems” (for example Dropbox, Microsoft 365, Google Drive) 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/academy will ensure that it is satisfied with controls put in place by remote / cloud based data services providers to protect the data.

As a Data Controller, the school is responsible for the security of any data passed to a “third party”. Specific data processing clauses must be included in all contracts where personal data is likely to be passed to a third party.

All paper based personal data must be held in lockable storage, whether on or off site.

### 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 local authority or other agencies. In these circumstances:

* Users may not remove or copy sensitive or restricted or protected personal data from the school/academy 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 (e.g. family members) when out of school/academy
* 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
* 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 (if relevant) in this event.

### Disposal of personal data

The school should implement a document retention schedule that defines the length of time personal data is held before secure destruction. The Information and Records Management Society [Toolkit for schools](http://irms.org.uk/page/SchoolsToolkit) provides support for this process. The school must ensure 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 disposed of, and other media must be shredded, incinerated or otherwise disintegrated.

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.

## C1 - 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)

|  |  |
| --- | --- |
| Web site(s) address/device | Reason for concern |
|  |  |
|  |  |
|  |  |

#### Conclusion and Action proposed or taken

|  |  |
| --- | --- |
|  |  |
|  |  |
|  |  |

##

|  |
| --- |
| C2 - Reporting LogGroup:  |
| Date | Time | Incident | Action Taken | Incident Reported By | Signature |
| What? | By Whom? |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
| Training Needs Audit LogGroup:  |
| Relevant training the last 12 months | Identified Training Need | To be met by | Cost | Review Date |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

##

## C3 – Summary of Legislation

Schools should be aware of the legislative framework under which this online 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 online 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.

School/academies may wish to view the National Crime Agency website which includes information about [“Cyber crime – preventing young people from getting involved”](https://www.nationalcrimeagency.gov.uk/what-we-do/crime-threats/cyber-crime/cyber-crime-preventing-young-people-from-getting-involved). Each region in England (& Wales) has a Regional Organised Crime Unit (ROCU) Cyber-Prevent team that works with schools to encourage young people to make positive use of their cyber skills. There is a useful [summary of the Act on the NCA site](https://nationalcrimeagency.gov.uk/who-we-are/publications/75-guide-to-the-computer-misuse-act/file).

### 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.

### The Data Protection Act 2018:

#### Updates the 1998 Act, incorporates the General Data Protection Regulations (GDPR) and aims to:

* Facilitate the secure transfer of information within the European Union.
* Prevent people or organisations from holding and using inaccurate information on individuals. This applies to information regarding both private lives or business.
* Give the public confidence about how businesses can use their personal information.
* Provide data subjects with the legal right to check the information businesses hold about them. They can also request for the data controller to destroy it.
* Give data subjects greater control over how data controllers handle their data.
* Place emphasis on accountability. This requires businesses to have processes in place that demonstrate how they’re securely handling data.
* Require firms to keep people’s personal data safe and secure. Data controllers must ensure that it is not misused.
* Require the data user or holder to register with the Information Commissioner.

#### All data subjects have the right to:

* Receive clear information about what you will use their data for.
* Access their own personal information.
* Request for their data to be revised if out of date or erased. These are known as the right to rectification and the right to erasure
* Request information about the reasoning behind any automated decisions, such as if computer software denies them access to a loan.
* Prevent or query about the automated processing of their personal data.

### 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, offensive, or threatening letter, electronic communication or other article to another person.

### Regulation of Investigatory Powers Act 2000

It is an offence for any person to intentionally and without lawful authority intercept any communication. 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.
* The school reserves the right to monitor its systems and communications in line with its rights under this act.

### 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).

### Telecommunications Act 1984

It is an offence to send a message or other matter that is grossly offensive or of an indecent, obscene or menacing character. It is also an offence to send a message that is intended to cause annoyance, inconvenience or needless anxiety to another that the sender knows to be false.

### Criminal Justice & Public Order Act 1994

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

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. Viewing an indecent image of a child on your computer means that you have made a digital image. An image of a child also covers pseudo-photographs (digitally collated or otherwise). A person convicted of such an offence may face up to 10 years in prison

### Sexual Offences Act 2003

A 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. Children, Families and Education Directorate page 38 April 2007.

### 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

These rights are not absolute. The school is obliged to respect these rights and freedoms, balancing 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.

51

### The Education and Inspections Act 2011

Extended the powers included in the 2006 Act and gave permission for Headteachers (and nominated staff) to search for electronic devices. It also provides powers to search for data on those devices and to delete data.

### The Protection of Freedoms Act 2012

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

### The School Information Regulations 2012

Requires schools to publish certain information on its website:

<https://www.gov.uk/guidance/what-maintained-schools-must-publish-online>

### Serious Crime Act 2015

Introduced new offence of sexual communication with a child. Also created new offences and orders around gang crime (including CSE)

### Criminal Justice and Courts Act 2015

Revenge porn – as it is now commonly known – involves the distribution of private and personal explicit images or video footage of an individual without their consent, with the intention of causing them embarrassment and distress. Often revenge porn is used maliciously to shame ex-partners. Revenge porn was made a specific offence in the Criminal Justice and Courts Act 2015. The Act specifies that if you are accused of revenge porn and found guilty of the criminal offence, you could be prosecuted and face a sentence of up to two years in prison.

For further guidance or support please contact the [Revenge Porn Helpline](https://revengepornhelpline.org.uk/)

### C4 - Links to other organisations or documents

The following links may help those who are developing or reviewing a school online safety policy and creating their online safety provision:

### UK Safer Internet Centre

Safer Internet Centre – <https://www.saferinternet.org.uk/>

South West Grid for Learning - h[ttps://swgfl.org.uk/products-services/online-safety/](http://www.swgfl.org.uk)

Childnet – <http://www.childnet-int.org/>

Professionals Online Safety Helpline - <http://www.saferinternet.org.uk/about/helpline>

Revenge Porn Helpline - https://revengepornhelpline.org.uk/

Internet Watch Foundation - <https://www.iwf.org.uk/>

Report Harmful Content - <https://reportharmfulcontent.com/>

### CEOP

CEOP - <http://ceop.police.uk/>

[ThinkUKnow](http://www.thinkuknow.co.uk/) - <https://www.thinkuknow.co.uk/>

### Others

[LGfL – Online Safety Resources](https://www.lgfl.net/online-safety/resource-centre?a=3)

[Kent – Online Safety Resources page](http://www.kelsi.org.uk/child-protection-and-safeguarding/e-safety/e-safety-classroom-materials)

INSAFE/Better Internet for Kids - <https://www.betterinternetforkids.eu/>

UK Council for Internet Safety (UKCIS) - <https://www.gov.uk/government/organisations/uk-council-for-internet-safety>

Netsmartz - <http://www.netsmartz.org/>

### Tools for Schools

Online Safety BOOST – <https://boost.swgfl.org.uk/>

360 Degree Safe – Online Safety self-review tool – <https://360safe.org.uk/>

360Data – online data protection self-review tool: [www.360data.org.uk](http://www.360data.org.uk)

SWGfL Test filtering - <http://testfiltering.com/>

UKCIS Digital Resilience Framework - <https://www.gov.uk/government/publications/digital-resilience-framework>

### Bullying/Online-bullying/Sexting/Sexual Harassment

Enable – European Anti Bullying programme and resources (UK coordination/participation through SWGfL & Diana Awards) - <http://enable.eun.org/>

SELMA – Hacking Hate - <https://selma.swgfl.co.uk>

Scottish Anti-Bullying Service, Respectme - <http://www.respectme.org.uk/>

Scottish Government - Better relationships, better learning, better behaviour - <http://www.scotland.gov.uk/Publications/2013/03/7388>

DfE - Cyberbullying guidance - <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/374850/Cyberbullying_Advice_for_Headteachers_and_School_Staff_121114.pdf>

Childnet – Cyberbullying guidance and practical PSHE toolkit:

<http://www.childnet.com/our-projects/cyberbullying-guidance-and-practical-toolkit>

[Childnet – Project deSHAME – Online Sexual Harrassment](http://www.childnet.com/our-projects/project-deshame)

[UKSIC – Sexting Resources](https://www.saferinternet.org.uk/advice-centre/teachers-and-professionals/teaching-resources/sexting-resources)

Anti-Bullying Network – <http://www.antibullying.net/cyberbullying1.htm>

[Ditch the Label – Online Bullying Charity](https://www.ditchthelabel.org/)

[Diana Award – Anti-Bullying Campaign](http://www.antibullyingpro.com/)

### Social Networking

Digizen – [Social Networking](http://digizen.org/socialnetworking/)

UKSIC - [Safety Features on Social Networks](http://www.saferinternet.org.uk/advice-and-resources/teachers-and-professionals/safety-features)

[Children’s Commissioner, TES and Schillings – Young peoples’ rights on social media](https://www.tes.com/teaching-resources/digital-citizenship)

### Curriculum

53

SWGfL Evolve - <https://projectevolve.co.uk>

[UKCCIS – Education for a connected world framework](https://www.gov.uk/government/groups/uk-council-for-child-internet-safety-ukccis)

Teach Today – [www.teachtoday.eu/](http://www.teachtoday.de/en/)

Insafe - [Education Resources](http://lreforschools.eun.org/web/guest/insafe)

### Data Protection

[360data - free questionnaire and data protection self review tool](http://360data.org.uk/)

[ICO Guides for Education (wide range of sector specific guides)](https://ico.org.uk/for-organisations/education/)

[DfE advice on Cloud software services and the Data Protection Act](https://www.gov.uk/government/publications/cloud-software-services-and-the-data-protection-act)

[IRMS - Records Management Toolkit for Schools](https://c.ymcdn.com/sites/irms.site-ym.com/resource/collection/8BCEF755-0353-4F66-9877-CCDA4BFEEAC4/2016_IRMS_Toolkit_for_Schools_v5_Master.pdf)

[NHS - Caldicott Principles (information that must be released)](https://www.igt.hscic.gov.uk/Caldicott2Principles.aspx)

[ICO Guidance on taking photos in schools](https://ico.org.uk/for-the-public/schools/photos/)

[Dotkumo - Best practice guide to using photos](http://campuspr.co.uk/wp-content/uploads/2017/10/Commissioning-original-photography.pdf)

### Professional Standards/Staff Training

[DfE – Keeping Children Safe in Education](https://www.gov.uk/government/publications/keeping-children-safe-in-education--2)

DfE - [Safer Working Practice for Adults who Work with Children and Young People](http://www.safeguardinginschools.co.uk/wp-content/uploads/2015/10/Guidance-for-Safer-Working-Practices-2015-final1.pdf%22%20%5Ct%20%22_blank)

[Childnet – School Pack for Online Safety Awareness](http://www.childnet.com/resources/school-pack-for-online-safety-awareness)

[UK Safer Internet Centre Professionals Online Safety Helpline](http://www.saferinternet.org.uk/helpline)

### Infrastructure/Technical Support

[UKSIC – Appropriate Filtering and Monitoring](https://www.saferinternet.org.uk/advice-centre/teachers-and-school-staff/appropriate-filtering-and-monitoring)

SWGfL Safety & [Security](https://swgfl.org.uk/resources/) Resources

Somerset - [Questions for Technical Support](https://www.somerset.org.uk/sites/edtech/eSafety/Leading/Questions%20for%20Technical%20Support%202018.pdf)

NCA – [Guide to the Computer Misuse Act](https://nationalcrimeagency.gov.uk/who-we-are/publications/75-guide-to-the-computer-misuse-act/file)

NEN –  [Advice and Guidance Notes](https://www.nen.gov.uk/advice/%22%20%5Ct%20%22_blank)

### Working with parents and carers

[Online Safety BOOST Presentations - parent’s presentation](http://www.swgfl.org.uk/boost)

[Vodafone Digital Parents Magazine](http://www.vodafone.com/content/parents/digital-parenting.html)

[Childnet Webpages for Parents & Carers](http://www.childnet.com/parents-and-carers)

[Get Safe Online - resources for parents](http://www.getsafeonline.org/nqcontent.cfm?a_id=1182)

[Teach Today - resources for parents workshops/education](http://www.teachtoday.de/en/%22%20%5Ct%20%22_blank)

[Internet Matters](https://www.internetmatters.org/)

### Prevent

[Prevent Duty Guidance](https://www.gov.uk/government/publications/prevent-duty-guidance)

[Prevent for schools – teaching resources](http://www.preventforschools.org/)

[NCA – Cyber Prevent](https://www.nationalcrimeagency.gov.uk/what-we-do/crime-threats/cyber-crime/cyber-crime-preventing-young-people-from-getting-involved)

Childnet – [Trust Me](https://www.childnet.com/resources/trust-me)

### Research

Ofcom –Media Literacy Research

Further links can be found at the end of the UKCIS [Education for a Connected World Framework](https://www.gov.uk/government/publications/education-for-a-connected-world)

**C5 - 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

**ICT Mark** - Quality standard for schools provided by NAACE INSET In Service Education and Training

**IP address -** The label that identifies each computer to other computers using the IP (internet protocol)

**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 to provide the safe broadband provision to schools across Britain.

**Ofcom -** Office of Communications (Independent communications sector regulator)

**TUK** - Think U Know – educational e-Safety programmes for schools, young people and parents.

**VLE** - Virtual Learning Environment (a software system designed to support teaching and learning in an educational setting.

**WAP** - Wireless Application Protocol

22

1. Authorised device – purchased by the pupil/family through a school-organised scheme. This device may be given full access to the network as if it were owned by the school. [↑](#footnote-ref-1)