



ysgol ardudwy



ysgol ardudwy

E-Safety Policy

Dyddiad Mabwysiadu : 24/10/18

Dyddiad Adolygu : 23/10/2021

Llofnod Cadeirydd y Corff Llywodraethol: *Anwen Hughes*

Dyddiad: 24/10/2018

Llofnod y Pennaeth:

H A Williams

Dyddiad: 24/10/2018

Contents

Introduction	1
Development/Monitoring/Review of this Policy	4
Roles and Responsibilities	5
Policy Statements	8
Communication Technologies	16
User Actions	18
Responding to incidents of misuse	19
Learner Actions	22
Staff Actions	23
Appendix	24
Appendices – Section A - Acceptable use agreement	25
Appendices – Section B – Specific Policies	25
Appendices – Section C – Supporting documents and links	25
A1 Learner acceptable use agreement template – for younger learners (Foundation)	27
A2 Learner acceptable use agreement (AUA) template – for older learners	28
A3 Staff (and volunteer) acceptable use agreement template	31
A4 Parent/carers acceptable use agreement template	34
A5 Acceptable use agreement for community users template	37
B1 Schooltechnical security policy template (including filtering and passwords)	38
B2 Schoolpersonal data handling policy template	46
B3 SchoolMobile Technologies Policy Template (inc. BYOD/BYOT)	59
B4 Social Media Template Policy	64
B5 Schoolpolicy template - Online safety group terms of reference	70
C1 Responding to incidents of misuse – flow chart	72
C2 Record of reviewing devices/internet sites	73
C3 Reporting Log Template	74
C4 Training Needs Audit Log Template	75
C5 Summary of Legislation	76
C6 Office 365 – further information	79
C7 Links to other organisations or documents	82
C8 Glossary of terms	85



ysgol ardudwy

Introduction

The online safety policy template

These Schoolonline safety policy templates are intended to help Schoolleaders produce a suitable online safety policy document which will consider all current and relevant issues, in a whole Schoolcontext, linking with other relevant policies, such as the safeguarding, behaviour and anti-bullying policies.

The requirement to ensure that learners are able to use the internet and related communications technologies appropriately and safely is addressed as part of the wider duty of care to which all who work in schools/colleges are bound. Schools/colleges must, through their online safety policy, meet their statutory obligations to ensure that learners are safe and are protected from potential harm, both on and off-site. The policy will also form part of the school's/college's protection from legal challenge, relating to the use of digital technologies.

These policy templates suggest policy statements which, in the view of Welsh Government, would be essential in any Schoolonline safety policy, based on good practice. In addition there are a range of alternative statements that schools/colleges should consider and choose those that are most suitable, given their particular circumstances.

An effective School online safety policy must be tailored to the needs of each School and an important part of the process will be the discussion and consultation which takes place during the writing or review of the policy. This will help ensure that the policy is owned and accepted by the whole Schoolcommunity.

It is suggested that consultation in the production of this policy should involve:

- Governors
- Teaching staff and support staff
- Learners
- Community users and any other relevant groups.

Due to the ever changing nature of digital technologies, it is best practice that the School reviews the online safety policy at least annually and, if necessary, more frequently in response to any significant new developments in the use of the technologies, new threats to online safety or incidents that have taken place.

Schools/colleges are subject to an increased level of scrutiny of their online safety practices by Estyn Inspectors during inspections. From 2015 there are additional duties under the Counter Terrorism and Securities Act 2015 which requires schools/colleges to ensure that children are safe from terrorist and extremist material on the internet.

Given the range of optional statements offered and the guidance notes provided, this template document is much longer than the resulting policy is likely to be. It is intended that, while covering a complicated and ever changing aspect of the work of the school/college, the resulting policy should be concise and easily understood, if it is to be effective and adopted by all.

The template uses a number of alternative terms, e.g. school/college, these need to be deleted as relevant.



ysgol ardudwy

Where sections in the template are written in ITALICS it is anticipated that schools/colleges would wish to carefully consider whether or not to include that section or statement in their completed policy.

The first part of this document (approximately 25 pages) provides a template for an overall online safety policy for the school/college. The appendices contain acceptable use agreement templates and more detailed, specific policy templates. It will be for schools/colleges to decide which of these documents they chose to amend and adopt.



ysgol ardudwy



Ysgol Ardudwy

Online Safety Policy



ysgol arduwy

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

Development/Monitoring/Review of this Policy

This online safety policy has been developed by a working group/committee made up of:

- *Headteacher/senior leaders*
- *Online safety officer/coordinator*
- *Staff – including practitioners//support staff/technical staff*
- *Governors*
- *Parents and carers*
- *Community users*

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

Schedule for Development/Monitoring/Review

This online safety policy was approved by the <i>Governing body/governors subcommittee</i> on:	<i>Insert date</i>
The implementation of this online safety policy will be monitored by the:	<i>E-safety coordinator</i>
Monitoring will take place at regular intervals:	<i>once a year</i>
The <i>Governing Body/governors subcommittee</i> 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:	<i>once a year</i>
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:	<i>07/01/2019</i>
Should serious online safety incidents take place, the following external persons/agencies should be informed:	<i>LA ICT manager, LA safeguarding officer, police</i>

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

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



ysgol ardudwy

Roles and Responsibilities

The following section outlines the online safety roles and responsibilities of individualsⁱ and groups within the school/college:

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 *Governing Body/governor's sub-committee* receiving regular information about online safety incidents and monitoring reports. A member of the Governing Body should take on the role of online safety governorⁱⁱ to include:

- regular meetings with the online safety co-ordinator/officer
- regular monitoring of online safety incident logs
- regular monitoring of filtering change control logs (where possible)
- reporting to relevant governors/sub-committee/meeting

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 may be delegated to the online safety co-ordinator/officer
- The headteacher and (at least) another member of the senior leadership team should be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff¹
- The headteacher/senior leaders are responsible for ensuring that the online safety co-ordinator/officer 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/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 support to those colleagues who take on important monitoring roles.
- The headteacher/senior leaders will receive regular monitoring reports from the online safety co-ordinator/officer.

Online safety co-ordinator/officer:

Ceri Murray

The online safety co-ordinator/officer

- 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 (or identifies sources of) training and advice for staff
- liaises with the local authority/relevant body
- liaises with (school/college) technical staff



ysgol ardudwy

- receives reports of online safety incidents² and creates a log of incidents to inform future online safety developments.
- meets regularly with online safety governor to discuss current issues, review incident logs and if possible, filtering change control logs
- attends relevant meeting/sub-committee of governors
- reports regularly to headteacher/senior leadership team

Network manager/technical staff:

Hywel Jones

The network manager/technical staff (or managed service provider) is responsible for ensuring:

- that the *School* technical infrastructure is secure and is not open to misuse or malicious attack
- that the School meets (as a minimum) the required online safety technical requirements as identified by the local authority or other relevant body and also the online safety policy/guidance that may apply.
- that users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed
- 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 the *network/internet/learning platform/Hwb/remote access/email* is regularly monitored in order that any misuse/attempted misuse can be reported to the *headteacher/senior leader; online safety co-ordinator/officer* for investigation/action/sanction
- *that (if present) monitoring software/systems are implemented and updated as agreed in School policies*
- *that the filtering policy (if one exists), is applied and updated on a regular basis and its implementation is not the sole responsibility of any single person (see appendix "Technical Security Policy Template" for good practice)*

Teaching and Support Staff

Are responsible for ensuring that:

- they have an up to date awareness of online safety matters and of the current School online safety policy and practices
- they have read, understood and signed the staff acceptable use agreement (AUA)
- they report any suspected misuse or problem to the *headteacher/senior leader; online safety co-ordinator/officer* for investigation/action
- all digital communications with learners/parents and 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
- Learners understand and follow the online safety and acceptable use agreements
- learners 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



ysgol ardudwy

- in lessons where internet use is pre-planned 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*

Designated senior person

Aled Williams

The designated senior person should be trained in online safety issues and be aware of the potential for serious safeguarding issues to arise from:

- sharing of personal data³
- access to illegal/inappropriate materials
- inappropriate online contact with adults/strangers
- potential or actual incidents of grooming
- cyber-bullying

Online safety group

The online safety group⁴ provides a consultative group that has wide representation from the school community, with responsibility for issues regarding online safety and monitoring the online safety policy including the impact of initiatives. Depending on the size or structure of the school this group may be part of the safeguarding group. The group will also be responsible for regular reporting to the Governing Body.

Members of the online safety group (or other relevant group) will assist the online safety co-ordinator/officer (or other relevant person, as above) with:

- the production/review/monitoring of the School online safety policy/documents.
- *the production/review/monitoring of the School filtering policy (if possible and if the School chooses to have one) and requests for filtering changes.*
- mapping and reviewing the online safety curricular provision – ensuring relevance, breadth and progression
- monitoring network/internet/incident logs where possible
- consulting stakeholders – including parents/carers and the learners about the online safety provision
- monitoring improvement actions identified through use of the 360 degree safe Cymru self review tool

An online safety group terms of reference template can be found in the appendices

Learners:

- are responsible for using the School digital technology systems in accordance with the learner 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 cyber-bullying.

³ See Personal Data Policy in the Appendix



ysgol ardudwy

- should understand the importance of adopting good online safety practice when using digital technologies out of School and realise that the school online safety policy covers their actions out of school/college, if related to their membership of the school/college

Parents and carers

Parents and carers play a crucial role in ensuring that their children understand the need to use the internet/mobile devices in an appropriate way. The School will take every opportunity to help parents understand these issues through *parents' evenings, newsletters, letters, website, Hwb, learning platform and information about national/local online safety campaigns/literature*. Parents and carers will be encouraged to support the School in promoting good online safety practice and to follow guidelines on the appropriate use of:

- digital and video images taken at School events
- access to parents' sections of the website, Hwb, learning platform and online learner records
- their children's personal devices in the School (where this is allowed)

Community Users

Community users who access School systems/website/Hwb/learning platform as part of the wider School provision will be expected to sign a community user AUA before being provided with access to School systems.

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 is therefore an essential part of the school/college's online safety provision. Learners 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: (Note: statements will need to be adapted, depending on School structure and the age of the learners)

- **A planned online safety curriculum across a range of subjects, (e.g. ICT/PSE/DCF) and topic areas and should be regularly revisited**
- **Key online safety messages should be reinforced as part of a planned programme of assemblies and tutorial/pastoral activities**
- **Learners should be taught in all lessons to be critically aware of the materials/content they access online 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.



ysgol ardudwy

- *Learners should be helped to understand the need for the learner acceptable use agreement and encouraged to adopt safe and responsible use both within and outside school/college*
- *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.*
- *It is accepted that from time to time, for good educational reasons, students may need to research topics, (e.g. racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the technical staff (or other nominated person) can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need.*

Education – parents and 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.

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

- *Curriculum activities*
- *Letters, newsletters, web site, learning platform, Hwb*
- *Parents and carers evenings/sessions*
- *High profile events/campaigns, e.g. Safer Internet Day*
- *Reference to the relevant web sites/publications, e.g. <https://hwb.wales.gov.uk/> www.saferinternet.org.uk/ <http://www.childnet.com/parents-and-carers> (see appendix for further links/resources)*

Education – the wider community

The School will provide opportunities for local community groups/members of the community to gain from the school/college's 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 School learning platform, Hwb, website will provide online safety information for the wider community
- Supporting community groups, e.g. early years settings, childminders, youth/sports/voluntary groups to enhance their online safety

Education and 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:



ysgol arduwy

- **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.** *It is expected that some staff will identify online safety as a training need within the performance management process.*
- **All new staff should receive online safety training as part of their induction programme, ensuring that they fully understand the Schoolonline safety policy and acceptable use agreements.**
- *The online safety co-ordinator/officer (or other nominated person) will receive regular updates through attendance at external training events, (e.g. from Consortium/SWGfL/LA/other relevant organisations) 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/INSET days.*
- *The online safety co-ordinator/officer (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 sub-committee/group involved in technology/online safety/health and safety/safeguarding . This may be offered in a number of ways:

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

Technical – infrastructure/equipment, filtering and monitoring

If the School has a managed ICT service provided by an outside contractor, it is the responsibility of the School to ensure that the managed service provider carries out all the online safety measures that would otherwise be the responsibility of the school/college, as suggested below. It is also important that the managed service provider is fully aware of the School online safety policy/acceptable use agreements. The School should also check their local authority/other relevant body policies on these technical issues if the service is not provided by the authority.

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

- **School technical systems will be managed in ways that ensure that the School meets recommended technical requirements**
- There will be regular reviews and audits of the safety and security of School technical systems
- Servers, wireless systems and cabling must be securely located and physical access restricted
- All users will have clearly defined access rights to Schooltechnical systems and devices.
- All users (at KS3 and above) will be provided with a username and secure password by *Hywel Jones* who will keep an up to date record of users and their usernames. Users are responsible for the security of their username and password *and will be required to change their password every 3 months.*



ysgol ardudwy

- The “master/administrator” passwords for the Schooldigital systems, used by the network manager (or other person) must also be available to the headteacher or other nominated senior leader and kept in a secure place, (e.g. Schoolsafe)
- [Hywel Jones](#) 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
- *The School has (if possible) provided enhanced/differentiated user-level filtering (allowing different filtering levels for different ages/stages and different groups of users: staff/learners, etc.).*
- Internet filtering should ensure that children are safe from terrorist and extremist material when accessing the internet.
- Where possible, School technical staff regularly monitor and record the activity of users on the School technical systems and users are made aware of this in the acceptable use agreement.
- An appropriate system is in place for users to report any actual/potential technical incident/security breach to the relevant person, as agreed).
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, mobile devices, etc., from accidental or malicious attempts which might threaten the security of the School systems and data. These are tested regularly. The School infrastructure and individual workstations are protected by up to date virus software.
- An agreed policy is in place (to be described) 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 (to be described) 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/college.
- An agreed policy is in place (to be described) that allows staff to/forbids staff from downloading executable files and installing programmes on School devices.
- An agreed policy is in place (to be described) regarding the use of removable media (eg memory sticks/CDs/DVDs) by users on School devices. Personal data cannot be sent over the internet or taken off the School site unless safely encrypted or otherwise secured. (see [School personal data policy template in the appendix for further detail](#))

Mobile technologies

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/college’s wireless network. The device then has access to the wider internet which may include the School learning platform and other cloud based services such as email and data storage.

All users should understand that the primary purpose of the use of mobile/personal devices in a School context is educational. The mobile technologies policy should be consistent with and inter-related to other relevant School policies including but not limited to those for safeguarding, behaviour, anti-bullying, acceptable use, and policies around theft or malicious damage. Teaching



ysgol ardudwy

about the safe and appropriate use of mobile technologies should be an integral part of the school/college's online safety education programme.

In preparing a mobile technologies policy the School should consider possible issues and risks. These may include: security risks in allowing connections to your School network; filtering of personal devices; breakages and insurance; access to devices for all learners; avoiding potential classroom distraction; network connection speeds, types of devices; charging facilities; total cost of ownership. A range of mobile technology implementations is possible.

For further reading, please refer to "Bring your own device: a guide for schools/colleges" by Alberta Education available at: <http://education.alberta.ca/admin/technology/research.aspx> and to the "NEN Technical Strategy Guidance Note 5 - Bring your own device" - <http://www.nen.gov.uk/bring-your-own-device-byod/>

A more detailed mobile technologies policy template can be found in the appendix. The School may however choose to include these aspects of their policy in a comprehensive acceptable use agreement, rather than in a separate mobile technologies policy. It is suggested that the School should in this overall policy document outline the main points from their agreed policy. A checklist of points to be considered in included below.

- The School acceptable use agreements for staff, learners, parents and carers will give consideration to the use of mobile technologies
- The School allows: (the School should complete the table below to indicate which devices are allowed and define their access to Schools systems)

	School Devices			Personal Devices		
	School owned for individual use	School owned for multiple users	Authorised device ⁵	Student owned	Staff owned	Staff owned
Allowed in school/college	/	/		No	yes	/
Full network access	/	/		No	No	/
Internet only				yes	yes	
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/out of school/college
- 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

⁵ Authorised device – purchased by the pupil/family through a school/college-organised scheme. This device may be given full access to the network as if it were owned by the school/college.



ysgol ardudwy

- 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/college
- Liability for damage
- Staff training

Personal devices:

- Which users are allowed to use personal mobile devices in School(staff/learners/visitors)
- Restrictions on where, when and how they may be used in school/college
- 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
- 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 and carers and learners need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for cyberbullying to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. It is common for employers to carry out internet searches for information about potential and existing employees. The School will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- **When using digital images, staff should inform and educate 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, eg., on social networking sites.**
- In accordance with guidance from the Information Commissioner's Office, parents/carers are welcome to take videos and digital images of their children at School events for their own personal use (as such use is not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published/made publicly available on social networking sites, nor should parents/carers comment on any activities involving other *learners* in the digital/video images.



ysgol ardudwy

- *Staff and volunteers are allowed to take digital/video images to support educational aims, but must follow School policies concerning the sharing, distribution and publication of those images. Those images should only be taken on School equipment, the personal equipment of staff should not be used for such purposes.*
- *Care should be taken when taking digital/video images that learners are appropriately dressed and are not participating in activities that might bring the individuals or the School 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.*
- *Written permission from parents or carers will be obtained before photographs of learners are published on the School website)*
- *Learners' work can only be published with the permission of the learner and parents or carers.*

Data Protection

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 which states that personal data must be:

- Fairly and lawfully processed
- Processed for limited purposes
- Adequate, relevant and not excessive
- Accurate
- Kept no longer than is necessary
- Processed in accordance with the data subject's rights
- Secure
- Only transferred to others with adequate protection.

The School must ensure that:

- It will hold the minimum personal data necessary to enable it to perform its function and it will not hold it for longer than necessary for the purposes it was collected for.
- Every effort will be made to ensure that data held is accurate, up to date and that inaccuracies are corrected without unnecessary delay.
- All personal data will be fairly obtained in accordance with the privacy notice and lawfully processed in accordance with the conditions for processing.
- policy (see appendix for policy template)
- It is registered as a data controller for the purposes of the Data Protection Act (DPA)
- Responsible persons are appointed/identified - senior information risk officer (SIRO) and information asset owners (IAOs)
- Risk assessments are carried out
- It has clear and understood arrangements for the security, storage and transfer of personal data
- Data subjects have rights of access and there are clear procedures for this to be obtained
- There are clear and understood policies and routines for the deletion and disposal of data



ysgol ardudwy

- There is a policy for reporting, logging, managing and recovering from information risk incidents
- There are clear data protection clauses in all contracts where personal data may be passed to third parties
- There are clear policies about the use of cloud storage/cloud computing which ensure that such data storage meets the requirements laid down by the Information Commissioner's Office.

Staff must ensure that they:

At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.

- Use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data.
- Transfer data using encryption and secure password protected devices.

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

- the data must be encrypted and password protected
- the device must be password protected
- the device must offer approved virus and malware checking software
- the data must be securely deleted from the device, in line with Schoolpolicy (below) once it has been transferred or its use is complete

Communications

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

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



ysgol ardudwy

Communication Technologies

	Staff & other adults			Learners				
	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	/							/
Use of mobile phones in lessons				/				/
Use of mobile phones in social time		/						/
Taking photos on mobile phones/cameras				/				/
Use of other mobile devices eg tablets, gaming devices	/				/	School		/
Use of personal email addresses in school/college, or on Schoolnetwork				/				/
Use of Schoolemail for personal emails		/						/
Use of messaging apps		/						/
Use of social media		/						/
Use of blogs				/				/

The School may also wish to add some of the following policy statements about the use of communications technologies, in place of, or in addition to the above table:

When using communication technologies the School considers the following as good practice:

- **The official School email service may be regarded as safe and secure and is monitored. Users should be aware that email communications are monitored. Staff and learners should therefore use only the School email service to communicate with others when in school/college, 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, chat, learning platform, etc.) must be professional in tone and content. These communications may only take place on official (monitored) School systems. Personal email addresses, text messaging or social media must not be used for these communications.**
- *Email addresses may be used at KS3 above will be provided with individual School email addresses for educational use.*



ysgol ardudwy

- *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 School website and only official email addresses should be used to identify members of staff.*

Social media

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

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

The School provides the following measures to ensure reasonable steps are in place to minimise risk of harm to 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

School staff should ensure that:

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

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



ysgol ardudwy

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, or impacts on, the School it must be made clear that the member of staff is not communicating on behalf of the School 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/college
- The School should effectively respond to social media comments made by others according to a defined policy or process

School use of social media for professional purposes will be checked regularly by the senior risk officer and online safety group to ensure compliance with the social media, data protection, communications, digital image and video policies.

Unsuitable/inappropriate activities

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

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

User Actions		Acceptable	Acceptable at certain times	Acceptable for nominated	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	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



ysgol arduwy

contain or relate to:	criminally racist material in UK – to stir up religious hatred (or hatred on the grounds of sexual orientation) - contrary to the Public Order Act 1986					X
	Pornography				X	
	promotion of any kind of discrimination				X	
	threatening behaviour, including promotion of physical violence or mental harm				X	
	Promotion of extremism or terrorism				X	
	any other information which may be offensive to colleagues or breaches the integrity of the ethos of the School or brings the School into disrepute				X	
Using School systems to run a private business					X	
Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the School					X	
Infringing copyright					X	
Revealing or publicising confidential or proprietary information, (e.g. financial/personal information, databases, computer/network access codes and passwords)					X	
Creating or propagating computer viruses or other harmful files					X	
Unfair usage (downloading/uploading large files that hinders others in their use of the internet)					X	
Online gaming (educational)			X			
Online gaming (non educational)					X	
Online gambling					X	
Online shopping/commerce				X		
File sharing					X	
Use of social media				X		
Use of messaging apps				X		
Use of video broadcasting, e.g. YouTube				X		

(The School should agree its own responses and place the ticks in the relevant columns, in the table above. They may also wish to add additional text to the column(s) on the left to clarify issues. The last section of the table has been left blank for schools/colleges to decide their own responses)

Responding to incidents of misuse

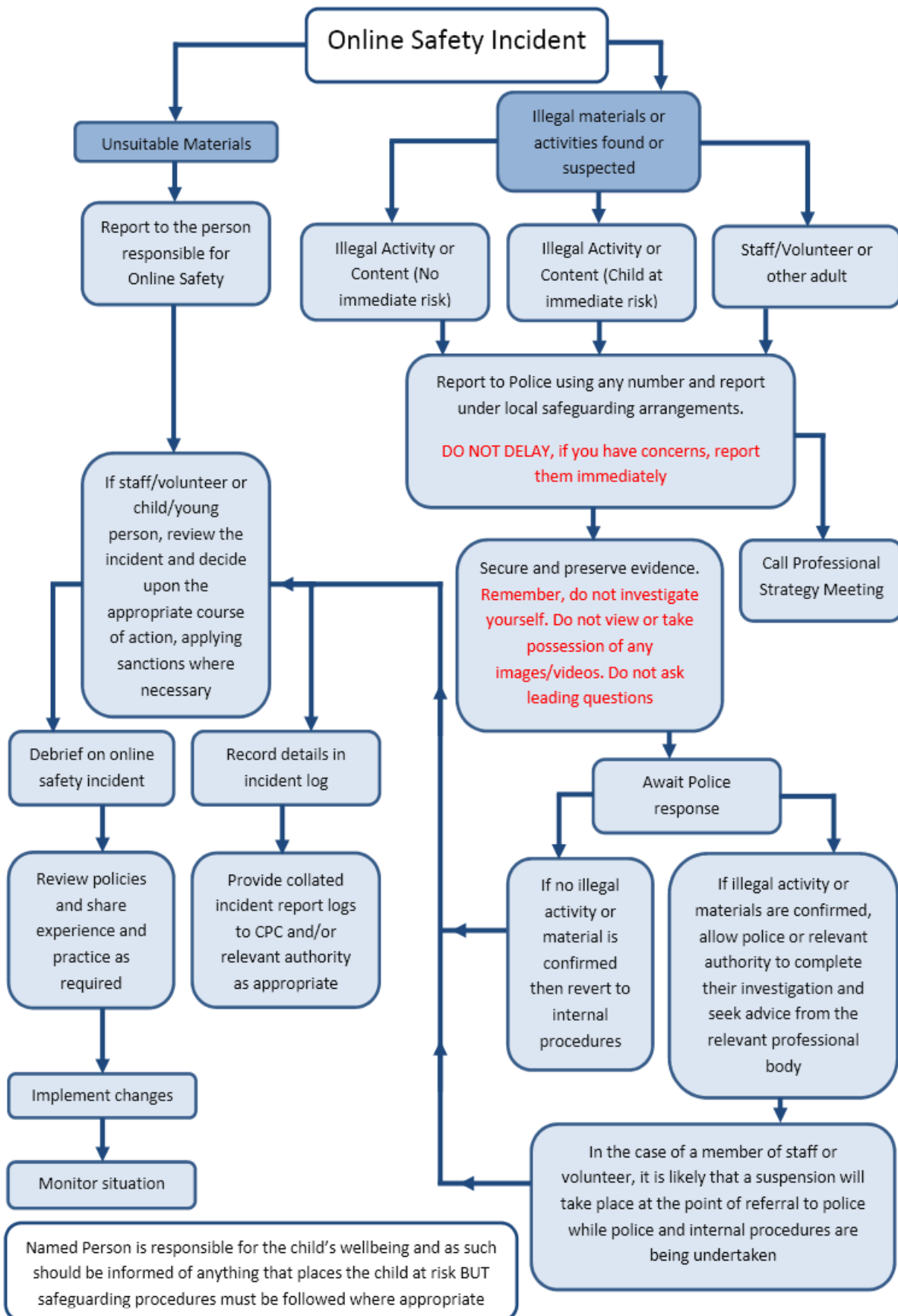
This guidance is intended for use when staff need to manage incidents that involve the use of online services. It encourages a safe and secure approach to the management of the incident. Incidents might involve illegal or inappropriate activities (see "User Actions" above).

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.



ysgol arduwy





ysgol ardudwy

Other Incidents

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

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

- Have more than one senior member of staff/volunteer involved in this process. This is vital to protect individuals if accusations are subsequently reported.
- Conduct the procedure using a designated computer that will not be used by learners 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
 - other criminal conduct, activity or materials
- Isolate the computer in question as best you can. Any change to its state may hinder a later police investigation.

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

School actions

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



ysgol arduwyl

Learner Actions

Incidents	Refer to class teacher/tutor	Refer to Head of Department/Head of 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 eg. detention/exclusion
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable/inappropriate activities).		X	X	X					
Unauthorised use of non-educational sites during lessons	X								
Unauthorised use of mobile phone/digital camera/other mobile device		X				X			
Unauthorised use of social media/messaging apps/personal email	X	X							
Unauthorised downloading or uploading of files	X	X							
Allowing others to access Schoolnetwork by sharing username and passwords		X				X	X		
Attempting to access or accessing the Schoolnetwork, using another learners' account			X			X	X		X
Attempting to access or accessing the Schoolnetwork, using the account of a member of staff			X			X	X		X
Corrupting or destroying the data of other users			X			X	X		X
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature			X			X			X
Continued infringements of the above, following previous warnings or sanctions			X			X			X
Actions which could bring the School into disrepute or breach the integrity of the ethos of the school/college			X	X		X			X
Using proxy sites or other means to subvert the school/college's filtering system			X			X	X		X
Accidentally accessing offensive or pornographic material and failing to report the incident		X						X	
Deliberately accessing or trying to access offensive or pornographic material			X	X		X	X		X



ysgol ardudwy

Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act			X					X	
---	--	--	---	--	--	--	--	---	--

Staff Actions

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



ysgol ardudwy

Deliberately accessing or trying to access offensive or pornographic material		X	X		X	X	X	X
Breaching copyright or licensing regulations		X				X		
Continued infringements of the above, following previous warnings or sanctions		X	X	X		X	X	X

Appendix

Copies of the more detailed template policies and agreements, contained in the appendix, can be downloaded from:

<https://hwb.wales.gov.uk>

Acknowledgements

Welsh Government and SWGfL would like to acknowledge a range of individuals and organisations whose policies, documents, advice and guidance have contributed to the development of this School online safety policy templates and of the 360 degree safe Cymru online safety self review tool:

- Members of the SWGfL online safety group
- Representatives of SW local authorities
- Representatives from a range of Welsh schools/colleges involved in consultation and pilot groups
- Plymouth University online safety

Copyright of these policy templates is held by SWGfL. Schools/colleges and other educational institutions are permitted free use of the policy templates for the purposes of policy review and development. Any person or organisation wishing to use the document for other purposes should seek consent from SWGfL (esafety@swgfl.org.uk) and acknowledge its use.

Every effort has been made to ensure that the information included in this document is accurate, as at the date of publication in December 2016. However, SWGfL cannot guarantee its accuracy, nor can it accept liability in respect of the use of the material.

© SWGfL 2017



ysgol ardudwy

Appendices – Section A - Acceptable use agreement

- A1 Learner Acceptable use agreement template (younger children)
- A2 Learner Acceptable use agreement template (older children)
- A3 Staff and Volunteers Acceptable use agreement template
- A4 Parents /Carers Acceptable use agreement template
- A5 Community Users Acceptable use agreement template

Appendices – Section B – Specific Policies

- B1 Technical Security Policy template
- B2 Personal Data Policy template
- B3 Mobile technologies policy template
- B4 Social media policy template
- B5 Online safety group terms of reference

Appendices – Section C – Supporting documents and links

- C1 Responding to incidents of misuse – flowchart
- C2 Record of reviewing sites (for internet misuse)
- C3 Reporting log template
- C4 Training needs audit template
- C5 Summary of legislation



ysgol ardudwy

- C6 Office 365 – further details
- C7 Links to other organisations and documents
- C8 Glossary of terms



ysgol ardudwy

A1 Learner acceptable use agreement template – for younger learners (Foundation)

This is how we stay safe when we use computers:

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

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

I will take care of the computer and other equipment

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

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

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

Signed (child):

Signed (parent):



ysgol ardudwy

A2 Learner acceptable use agreement (AUA) template – for older learners

Sections that include advice or guidance are written in BLUE. It is anticipated that schools/colleges will remove these sections from their final AUA document. Schools/colleges should review and amend the contents of this AUA to ensure that it is consistent with their online safety policy and other relevant School policies. Due to the number of optional statements and the advice/guidance sections included in this template, it is anticipated that the final AUA will be more concise.

School policy

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

This Acceptable use agreement is intended to ensure:

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

The School will try to ensure that learners will have good access to digital technologies to enhance their learning and will, in return, expect the learners 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 the School will monitor my use of systems, devices and digital communications
- I will keep my username and password safe and secure – I will not share it, nor will I try to use any other person's username and password. I 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 online
- I will not disclose or share personal information about myself or others when online (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 online, 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 online.

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

- I understand that the School systems and devices are primarily intended for educational use and that I will only use them for personal or recreational use if I have permission



ysgol ardudwy

- I will only make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work, if I have permission
- I will only use the School systems or devices for online gaming, online gambling, internet shopping, file sharing, or video broadcasting (eg YouTube), if I have permission of a member of staff to do so.

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

- I will respect others' work and property and will only access, copy, remove or alter any other user's files, with 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 only take or distribute images of others with their permission.

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

- I will only use my own personal device(s) in School if I have permission I understand that, if I do use my own device(s) in the school/college, 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 only open hyperlinks in emails or attachments to emails, if I know and trust the person/organisation who sent the email, and have no concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes)
- I will only install/ store programmes on a School device, if I have permission
- I will only use social media sites with permission and at the times that are allowed

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

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

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

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

Please complete the sections below / 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



ysgol ardudwy

not sign and return this agreement, access will not be granted to School systems and devices.

Learner acceptable use agreement form

This form relates to the learner 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 the School systems and devices (both in and out of school/college)
- I use my own devices in the School(when allowed), e.g. mobile phones, gaming devices, cameras etc
- I use my own equipment out of the School in a way that is related to me being a member of this school/college, e.g. communicating with other members of the school/college, accessing School email, learning platform, website, etc.

Name of Learner:

Group/Class

Signed:

Date:

Parent/Carer Countersignature

Name of parent / carer

signature Date



ysgol ardudwy

A3 Staff (and volunteer) acceptable use agreement template

School policy

New technologies have become integral to the lives of children and young people in today's society, both within schools/colleges and in their lives outside school/college. The internet and other digital 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 safer internet access at all times.

This acceptable use agreement is intended to ensure:

- that staff and volunteers will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- that School 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 digital technologies in their everyday work.

The School will try to ensure that staff and volunteers will have good access to digital technologies to enhance learning opportunities and will, in return, expect staff and volunteers to agree to be responsible users.

Acceptable use agreement

I understand that I must use School digital technologies 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 ICT for enhancing learning and will ensure that learners receive opportunities to gain from the use of digital technologies. I will, where possible, educate the young people in my care in the safe use of ICT and embed online safety in my work with young people.

For my professional and personal safety:

- I understand that the School will monitor my use of the ICT systems, email and other digital communications.
- I understand that the rules set out in this agreement also apply to use of School ICT systems (e.g. laptops, email, VLE etc.) out of school/college, 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/college.
- 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.



ysgol ardudwy

- I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person.

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

- I will only access, copy, remove or alter any other user's files, with 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 only use my personal equipment to record these images, if I have permission to do so. Where these images are published, (e.g. on the School website/learning platform) it will not be possible to identify by name, or other personal information, those who are featured.
- I will only use chat and social networking sites in School in accordance with the school/college's policies. (schools/colleges should amend this section to take account of their policy on access to social networking and similar sites)
- 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 online activity that may compromise my professional responsibilities.

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

- When I use my mobile devices (laptops/mobile phones/USB devices etc) in school/college, I will follow the rules set out in this agreement, in the same way as if I was using School equipment. I will also follow any additional rules set by the School about such use. I will ensure that any such devices are protected by up to date anti-virus software and are free from viruses.
- I will not use personal email addresses on the School digital technology 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 policies.
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, extremist material or 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 only make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work, with permission
- I will only install or attempt to install/store programmes on devices or if this is allowed in School policies.
- I will not disable or cause any damage to School equipment, or the equipment belonging to others.



ysgol ardudwy

- I will only transport, hold, disclose or share personal information about myself or others, as outlined in the school/college/LA Personal data policy (or other relevant policy). Where digital personal data is transferred outside the secure local network, it must be encrypted. Paper based protected and restricted data must be held in lockable storage.
- I understand that data protection policy requires that any staff or learner data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by School policy to disclose such information to an appropriate authority.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.

When using the internet in my professional capacity or for School sanctioned personal use:

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

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

- I understand that this acceptable use agreement applies not only to my work and use of School digital technology equipment in school/college, but also applies to my use of School 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/college.
- 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/college) and my own devices (in School and when carrying out communications related to the school/college) within these guidelines.

Staff/Volunteer Name:

Signed:

Date:



ysgol ardudwy

A4 Parent/carer acceptable use agreement template

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

This Acceptable Use Policy is intended to ensure:

- that young people will be responsible users and stay safe while using the internet and other digital technologies for educational, personal and recreational use.
- that School systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that parents and carers are aware of the importance of online safety and are involved in the education and guidance of young people with regard to their online behaviour.

The School will try to ensure that *learners* will have good access to digital technologies to enhance their learning and will, in return, expect the *learners* to agree to be responsible users. A copy of the Learner Acceptable use agreement is attached to this permission form, so that parents/carers will be aware of the School expectations of the young people in their care.

Parents are requested to sign the permission form below to show their support of the School in this important aspect of the school's/college's work.

Permission Form

Parent/Carers Name: Learner's Name

As the parent/carer of the above learner(s), I give permission for my son/daughter to have access to the internet and to digital technology systems at school/college.

I know that my son/daughter has signed an acceptable use agreement and has received, or will receive, online safety education to help them understand the importance of safe use of technology and the internet – both in and out of school/college. .

I understand that the School will take every reasonable precaution, including applying monitoring and filtering systems, to ensure that young people will be safe when they use the internet and digital technology systems. I also understand that the School cannot ultimately be held responsible for the nature and content of materials accessed on the internet and using mobile technologies.

I understand that my son's/daughter's activity on the digital technology systems will be monitored and that the School will contact me if they have concerns about any possible breaches of the acceptable use agreement.

I will encourage my child to adopt safe use of the internet and digital technologies at home and will inform the School if I have concerns over my child's online safety.

Signed Date:



ysgol ardudwy

Use of Digital/Video Images

The use of digital/video images plays an important part in learning activities. Learners and members of staff may use digital cameras to record evidence of activities in lessons and out of school/college. These images may then be used in presentations in subsequent lessons.

Images may also be used to celebrate success through their publication in newsletters, on the School website and occasionally in the public media,

The School will comply with the Data Protection Act and request parents/carers permission before taking images of members of the school/college. We will also ensure that when images are published that the young people cannot be identified by the use of their names.

In accordance with guidance from the Information Commissioner's Office, parents/carers are welcome to take videos and digital images of their children at School events for their own personal use (as such use is not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published/made publicly available on social networking sites, nor should parents/carers comment on any activities involving other learners in the digital/video images.

Parents/carers are requested to sign the permission form below to allow the School to take and use images of their children and for the parents/carers to agree.

Digital/Video Images Permission Form

Parent/Carers Name:

Learners Names:

As the parent/carer of the above learner(s), I agree to the School taking and using digital/video images of my child/children. I understand that the images will only be used to support learning activities or in publicity that reasonably celebrates success and promotes the work of the school/college.

Yes/No

I agree that if I take digital or video images at, or of, – School events which include images of children, other than my own, I will abide by these guidelines in my use of these images.

Yes/No

Signed Date:



ysgol ardudwy

Use of Biometric Systems

If the School uses biometric systems (eg fingerprint/palm recognition technologies) to identify children for access, attendance recording, charging, library lending etc it must (under the "Protection of Freedoms" legislation) seek permission from a parent or carer. It is also recommended that they obtain this permission through the normal internet use permission/acceptable use agreement. Schools/colleges may therefore wish to add a section such as that below to this permission form.

The School uses biometric systems for the recognition of individual children in the following ways (the School should describe here how it uses the biometric system).

Biometric technologies have certain advantages over other automatic identification systems as pupils do not need to remember to bring anything with them so nothing can be lost, such as a swipe card.

The School has carried out a privacy impact assessment and is confident that the use of such technologies is effective and justified in a School context.

No complete images of **fingerprints/palms** are stored and the original image cannot be reconstructed from the data. That is, it is not possible for example, to recreate a pupil's fingerprint or even the image of a fingerprint from what is in effect a string of numbers.

Parents/carers are asked for permission for these biometric technologies to be used by their child:

Parent/Carers Name:

Learner(s) Names:

As the parent/carers of the above learner(s), I agree to the School using biometric recognition systems, as described above. I understand that the images cannot be used to create a whole fingerprint/palm print of my child and that these images will not be shared with anyone outside the school/college.

Yes/No

Signed Date:

Learner acceptable use agreement

On the following pages we have copied, for the information of parents and carers, the learner acceptable use agreement.



ysgol ardudwy

A5 Acceptable use agreement for community users template

This acceptable use agreement is intended to ensure:

- that community users of School digital technologies will be responsible users and stay safe while using these systems and devices.
- that School systems, devices and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that users are protected from potential risk in their use of these systems and devices.

Acceptable use agreement

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

This agreement will also apply to any personal devices that I bring into the School

- I understand that my use of School systems and devices and digital communications will be monitored
- I will not use a personal device that I have brought into School for any activity that would be inappropriate in a School setting.
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, 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 immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person.
- I will not access, copy, remove or otherwise alter any other user's files, without permission.
- I will ensure that if I take and/or publish images of others I will only do so with their permission. I will not use my personal equipment to record these images, without permission. If images are published it will not be possible to identify by name, or other personal information, those who are featured.
- I will not publish or share any information I have obtained whilst in the School on any personal website, social networking site or through any other means, unless I have permission from the school/college.
- I will not, without permission, 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 School device, nor will I try to alter computer settings, unless I have permission to do so.
- I will not disable or cause any damage to School equipment, or the equipment belonging to others.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.
- I will ensure that I have permission to use the original work of others in my own work



ysgol ardudwy

- Where work is protected by copyright, I will not download or distribute copies (including music and videos).
- I understand that if I fail to comply with this Acceptable Use Agreement, the School has the right to remove my access to School systems/devices

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

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/college's policies).
- access to personal data is securely controlled in line with the school/college'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.

If the School has an externally managed ICT service, it is the responsibility of the School to ensure that the managed service provider carries out all the online safety measures that might otherwise be carried out by the School itself (as suggested below). It is also important that the managed service provider is fully aware of the School online safety policy/ acceptable use agreements. The School should also check their local authority/other relevant body policies/guidance on these technical issues if the managed service is not provided by the authority.

Responsibilities

The management of technical security will be the responsibility of [Hywel Jones](#)

Technical Security

Policy statements

The School will be responsible for ensuring that the School infrastructure/network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also



ysgol arduwy

need to ensure that the relevant people will receive guidance and training and will be effective in carrying out their responsibilities:

- **School technical systems will be managed in ways that ensure that the School meets recommended technical requirements** (if not managed by the Local Authority, these may be outlined in Local Authority/other relevant body technical/Online safety policy and guidance)
- There will be regular reviews and audits of the safety and security of School technical systems
- Servers, wireless systems and cabling must be securely located and physical access restricted
- Appropriate security measures are in place to protect the servers, firewalls, switches, routers, wireless systems, work stations, mobile devices etc from accidental or malicious attempts which might threaten the security of the School systems and data.
- Responsibilities for the management of technical security are clearly assigned to appropriate and well trained staff
- All users will have clearly defined access rights to School technical systems. *Details of the access rights available to groups of users will be recorded by the network manager/technical staff/other person and will be reviewed, at least annually, by the online safety group.*
- Users will be made responsible for the security of their username and password, must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security.
- [Hywel Jones](#) is responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations
- *Mobile device security and management procedures are in place*
- *School/college/local authority/managed service provider/technical staff regularly monitor and record the activity of users on the School technical systems and users are made aware of this in the acceptable use agreement.*
- *Remote management tools are used by staff to control workstations and view users activity*
- *An appropriate system is in place for users to report any actual/potential technical incident to the online safety co-ordinator/network manager/technician (or other relevant person, as agreed).*
- An agreed policy is in place for the provision of temporary access of "guests", (e.g. trainee teachers, supply teachers, visitors) onto the School system.
- *An agreed policy is in place regarding the downloading of executable files and the installation of programmes on School devices by users*
- *An agreed policy is in place 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/college.*
- An agreed policy is in place regarding the use of removable media (eg memory sticks/CDs/DVDs) by users on School devices.
- The School infrastructure and individual workstations are protected by up to date software to protect against malicious threats from viruses, worms, trojans etc.
- Personal data cannot be sent over the internet or taken off the School site unless safely encrypted or otherwise secured.



ysgol ardudwy

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:

- All users will have clearly defined access rights to School technical systems and devices. Details of the access rights available to groups of users will be recorded by the Network Manager (or other person) and will be reviewed, at least annually, by the online safety group (or other group).
- **All School networks and systems will be protected by secure passwords that are regularly changed**
- **The “master/administrator” passwords for the School systems, used by the technical staff must also be available to the headteacher or other nominated senior leader and kept in a secure place eg School safe. Consideration should also be given to using two factor authentication for such accounts.**
- *Passwords for new users, and replacement passwords for existing users will be allocated by Hywel Jones. Any changes carried out must be notified to the manager of the password security policy (above).*
- All users (adults and young people) will have responsibility for the security of their username and password, must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security.
- *Users will change their passwords at regular intervals – as described in the staff and learner sections below.*
- *requests for password changes should be authenticated by (the responsible person) to ensure that the new password can only be passed to the genuine user (the School will need to decide how this can be managed – possibly by requests being authorised by a line manager for a request by a member of staff or by a member of staff for a request by a pupil/student)*

Staff passwords:

- **All staff users will be provided with a username and password** by Hywel Jones who will keep an up to date record of users and their usernames.



ysgol ardudwy

- for best practice, the password should be a minimum of 8 characters long and must include three of – uppercase character, lowercase character, number, special characters
- must not include proper names or any other personal information about the user that might be known by others
- for best practice, the account should be “locked out” following six successive incorrect log-on attempts
- temporary passwords e.g. used with new user accounts or when users have forgotten their passwords, shall be enforced to change immediately upon the next account log-on
- passwords shall not be displayed on screen, and shall be securely hashed (use of one-way encryption)
- passwords should be different for different accounts, to ensure that other systems are not put at risk if one is compromised and should be different for systems used inside and outside of school/college
- for best practice, should be changed at least every 60 to 90 days
- should not re-used for 6 months and be significantly different from previous passwords created by the same user - the last four passwords cannot be re-used .
- should be different for different accounts, to ensure that other systems are not put at risk if one is compromised
- should be different for systems used inside and outside of School

Learner passwords:

- **All users (at KS3 and above) will be provided with a username and password** by (insert name or title) who will keep an up to date record of users and their usernames.
- Users will be required to change their password every (insert period).
- Learners will be taught the importance of password security
- The complexity (ie minimum standards) will be set with regards to the cognitive ability of the children.

Schools/colleges may wish to add to this list for all or some learners any of the relevant policy statements from the staff section above.

Training/Awareness:

Members of staff will be made aware of the school/college’s password policy:

- at induction
- through the school/college’s online safety policy and password security policy
- through the acceptable use agreement

Pupils/students will be made aware of the school’s password policy:

- in lessons
- through the acceptable use agreement

Audit/Monitoring/Reporting/Review:

The responsible person Hywel Jones will ensure that full records are kept of:

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



ysgol ardudwy

Filtering

Introduction

The filtering of internet content provides an important means of preventing users from accessing material that is illegal or is inappropriate in an educational context. The filtering system cannot, however, provide a 100% guarantee that it will do so, because the content on the web changes dynamically and new technologies are constantly being developed. It is important, therefore, to understand that filtering is only one element in a larger strategy for 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/college.

Responsibilities:

The responsibility for the management of the school/college's filtering policy will be held by (insert title). 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
- *either... be reported to and authorised by a second responsible person prior to changes being made*
- *or... be reported to a second responsible person in the form of an audit of the change control logs*
- *be reported to the online safety group in the form of an audit of the change control logs*

All users have a responsibility to report immediately to Ceri Murray o'r Hywel Jones any infringements of the school's/college'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/college. Illegal content is filtered by broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list and other illegal content lists. Filter content lists are regularly updated and internet use is logged and frequently monitored. Ideally, the monitoring process alerts the School to breaches of the filtering policy, which are then acted upon. There is a clear route for reporting and managing changes to the filtering system. Where personal mobile devices are allowed internet access through the School network, filtering will be applied that is consistent with School practice.



ysgol ardudwy

- *Either - The School maintains and supports the managed filtering service provided by the internet service provider (ISP) (or other filtering service provider)*
- *and/or – the School manages its own filtering service*
- *the School has provided enhanced/differentiated user-level filtering through the use of the (insert name) filtering programme.*
- *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 Headteacher/Principal (or other nominated senior leader).*
- *mobile devices that access the School internet connection (whether School or personal devices) will be subject to the same filtering standards as other devices on the School systems*
- *any filtering issues should be reported immediately to the filtering provider.*
- *requests from staff for sites to be removed from the filtered list will be considered by the technical staff or Service Provider .If the request is agreed, this action will be recorded and logs of such actions shall be reviewed regularly by the online safety group.*

Education/Training/Awareness:

Learners 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:

- how, and to whom, users may request changes to the filtering (whether this is carried out in School or by an external filtering provider)
- the grounds on which they may be allowed or denied (schools may choose to allow access to some sites, e.g. social networking sites for some users, at some times, or for a limited period of time. There should be strong educational reasons for changes that are agreed).
- how a second responsible person will be involved to provide checks and balances (preferably this will be at the time of request, but could be retrospectively through inspection of records/audit of logs)
- any audit/reporting system.

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 [Hywel Jones](#) 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



ysgol ardudwy

indicated in the School online safety policy and the acceptable use agreements. *Monitoring will take place as follows:*

Audit/Reporting:

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

- *the second responsible person* [Ceri Murray/ Aled Williams](#)
- *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:

Schools/colleges may wish to seek further guidance. The following is recommended:

- NEN Technical guidance: <http://www.nen.gov.uk/advice/266/nen-guidance-notes.html>
- NEN Technical guidance: <http://www.nen.gov.uk/e-security-managing-and-maintaining-e-security/cyber-security-in-schools/colleges/>
- Somerset Guidance for schools/colleges – this checklist is particularly useful where a School uses external providers for its technical support/security: <http://www.360safe.org.uk/Files/Documents/Questions-for-Technical-Support-Somerset.aspx>
- Prevent duty - schools/colleges in England (and Wales) are required "to ensure children are safe from terrorist and extremist material when accessing the internet in school/college, including by establishing appropriate levels of filtering" ([Revised Prevent Duty Guidance: for England and Wales, 2015](#)).
- In response to the above, the UK Safer Internet Centre produced guidance for schools on "[Appropriate filtering and appropriate monitoring](#)".



ysgol ardudwy



ysgol ardudwy

B2 School personal data handling policy template

Suggestions for use

Sections within this template are for information or guidance purposes only are shown in **blue**. It is anticipated that schools/colleges would remove these sections from their completed policy document, though this will be a decision for the group that produces the policy.

Where sections in the template are written in *ITALICS* it is anticipated that schools/colleges would wish to consider whether or not to include that section or statement in their completed policy.

Where sections are highlighted in **BOLD** text, it is the view of the Welsh Government that these would be an essential part of a School online safety policy.

Recent publicity about data breaches suffered by organisations and individuals has made the area of personal data protection compliance a current and high profile issue for schools/colleges and other organisations. It is important that the School has a clear and well understood personal data handling policy in order to avoid or at least minimise the risk of personal data breaches. A breach may arise from a theft, a deliberate attack on your systems, the unauthorised 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 any data breach, particularly as the impact of data loss on individuals can be severe and cause extreme embarrassment, put individuals at risk and affect personal, professional or organisational reputation
- schools/colleges 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 any personal data breach.
- the School is subject to a wide range of legislation related to data protection and data use, with significant penalties for failure to observe the relevant legislation.

It is a statutory requirement for all schools/colleges to have a Data Protection Policy.

Schools/colleges have always held personal data on the pupils in their care, and increasingly this data is held digitally and accessible not just in School but also from remote locations. Legislation covering the safe handling of this data is mainly the Data Protection Act 1998 ('the DPA'). Moreover, following a number of losses of sensitive data, a report was published by the Cabinet Office in June 2008, Data Handling Procedures in Government. The latter stipulates the procedures that all departmental and public bodies should follow in order to maintain security of data. Given the personal and sensitive nature of much of the data held in schools/colleges, it is critical that they adopt these procedures too.

It is important to stress that the personal data handling policy template applies 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/colleges will need to carefully review this policy template and amend sections, as necessary, in the light of pertinent local authority regulations and guidance, and changes in legislation.



ysgol ardudwy

Data Protection Act

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

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

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

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

The Information Commissioners Office has produced a report aimed at helping schools/colleges meet their data protection obligations; you can read the report detailing data protection advice for schools/colleges – [ICO Guidance we gave to schools 2012](#) and a simple summary of the Data protection laws – [ICO Guide to data protection for organisations](#)



ysgol ardudwy

School personal data handling policy

Introduction

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

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

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

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

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

Policy Statements

The School will hold the minimum personal data necessary to enable it to perform its function and it will not hold it for longer than necessary for the purposes it was collected for.

Every effort will be made to ensure that data held is accurate, up to date and that inaccuracies are corrected without unnecessary delay.

All personal data will be fairly obtained in accordance with the "Privacy notice" and lawfully processed in accordance with the "Conditions for processing".

Personal Data

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

- Personal information about members of the School community – including learners, members of staff and parents/carers, e.g., names, addresses, contact details, legal guardianship contact details, health records, disciplinary records
- Curricular/academic data eg class lists, pupil/student progress records, reports, references
- Professional records, e.g., employment history, taxation and national insurance records, appraisal records and references



ysgol ardudwy

- Any other information that might be disclosed by parents/carers or by other agencies working with families or staff members.

Responsibilities

The school/college's Senior information risk officer (SIRO) is [Aled Williams](#). This person will keep up to date with current legislation and guidance and will:

- determine and take responsibility for the school/college's information risk policy and risk assessment
- appoint the Information asset owners (IAOs)

The School will identify Information asset owners (IAOs) for the various types of data being held (eg learner/staff/information/assessment data etc). The IAOs will manage and address risks to the information and will understand:

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

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

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

Registration

The School is registered as a Data controller on the Data protection register held by the Information Commissioner.

Information to parents and carers – the "Privacy Notice"

In order to comply with the fair processing requirements of the DPA, the School will inform parents and carers of all learners of the data they collect, process and hold on the pupils/students, 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 and carers through Parents/carers of young people who are new to the School will be provided with the privacy notice through

Training & awareness

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

- induction training for new staff
- staff meetings/briefings/Inset
- day to day support and guidance from Information asset owners



ysgol arduwy

Risk Assessments

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

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

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

Risk ID	Information asset affected	Information asset owner	Protective marking (Impact level)	Likelihood	Overall risk level (low, medium, high)	Action(s) to minimise risk

Impact Levels and protective marking

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

The School will ensure that all School staff, independent contractors working for it, and delivery partners, comply with restrictions applying to the access to, handling and storage of data classified as Protect, Restricted or higher. Unmarked material is considered 'unclassified'. The term 'UNCLASSIFIED' or 'NON' or 'NOT PROTECTIVELY MARKED' may be used to indicate positively that a protective marking is not needed.

All documents (manual or digital) that contain protected or restricted data will be labelled clearly with the impact level shown in the header and the release and destruction classification in the footer.



ysgol ardudwy

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

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

Secure storage of and access to data

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

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

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

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

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

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

- the data must be encrypted and password protected,
- the device must be password protected
- the device must offer approved virus and malware checking software and
- the data must be securely deleted from the device, in line with School policy (below) once it has been transferred or its use is complete.

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

The School has clear policy and procedures for the use of "Cloud Based Storage Systems" (for example Office365) and is aware that data held in remote and cloud storage is still required to be protected in line with the Data Protection Act. The School will ensure that it is satisfied with controls put in place by remote/cloud based data services providers to protect the data.



ysgol ardudwy

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

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

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

Secure transfer of data and access out of School

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

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

Disposal of data

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

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



ysgol arduwy

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

Audit logging/reporting/incident handling

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

The School has a policy for reporting, managing and recovering from information risk incidents, which establishes: (schools/colleges should determine their own reporting policy, in line with that of their LA (if relevant), and add details here)

- a "responsible person" for each incident
- a communications plan, including escalation procedures
- and results in a plan of action for rapid resolution; and
- a plan of action of non-recurrence and further awareness raising.

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

Use of technologies and protective marking

The following provides a useful guide:

	The information	The technology	Notes on Protect Markings (Impact Level)
Schoollife and events	Schoolterms, holidays, training days, the curriculum, extra-curricular activities, events, displays of pupils work, lunchtime menus, extended services, parent consultation events	Common practice is to use publically accessible technology such as Schoolwebsites or portal, emailed newsletters, subscription text services	Most of this information will fall into the NOT PROTECTIVELY MARKED (Impact Level 0) category.
Learning and achievement	Individual pupil/student academic, social and behavioural achievements, progress with learning, learning behaviour, how parents can support their child's learning, assessments, attainment, attendance, individual and	Typically schools/colleges will make information available by parents logging on to a system that provides them with appropriately secure access, such as a Learning Platform or portal, or by communication to a personal device or email	Most of this information will fall into the PROTECT (Impact Level 2) category. There may be learners whose personal data requires a RESTRICTED marking (Impact Level 3) or higher. For example, the home address of a child at risk. In this case,



ysgol ardudwy

	personalised curriculum and educational needs.	account belonging to the parent.	the School may decide not to make this pupil/student record available in this way.
Messages and alerts	Attendance, behavioural, achievement, sickness, School closure, transport arrangements, and other information that it may be important to inform or contact a parent about as soon as possible. This may be particularly important when it is necessary to contact a parent concerning information that may be considered too sensitive to make available using other online means.	Email and text messaging are commonly used by schools/colleges to contact and keep parents informed. Where parents are frequently accessing information online then systems e.g. Learning Platforms or portals, might be used to alert parents to issues via "dashboards" of information, or be used to provide further detail and context.	Most of this information will fall into the PROTECT (Impact Level 1) category. However, since it is not practical to encrypt email or text messages to parents, schools/colleges should not send detailed personally identifiable information. General, anonymous alerts about schools/colleges closures or transport arrangements would fall into the NOT PROTECTIVELY MARKED (Impact Level 0) category.

Appendices: Additional issues/documents related to personal data handling in schools/colleges:

Use of Biometric Information

The Protection of Freedoms Act 2012, includes measures that affect schools and colleges that use biometric recognition systems, such as fingerprint identification and facial scanning:

- for all pupils in schools and colleges under 18, they must obtain the written consent of a parent before they take and process their child's biometric data.
- they must treat the data with appropriate care and must comply with data protection principles as set out in the Data Protection Act 1998.
- they must provide alternative means for accessing services where a parent or pupil has refused consent.

Schools/colleges may wish to consider these changes when reviewing their Personal Data Handling Template. Schools/colleges may wish to incorporate the parental permission procedures into existing parental forms, (e.g., AUA/Digital and video images permission form).



ysgol ardudwy

Freedom of Information

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

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

A summary of good practice in dealing with requests and details of model publication schemes can be found on the ICO website – [ICO guidance for-organisations/guide-to-freedom-of-information/publication-scheme/](https://ico.org.uk/for-organisations/guide-to-freedom-of-information/publication-scheme/)

Freedom of Information Act

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

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

Model Publication Scheme

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

Safeguarding

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

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



ysgol ardudwy

Criminal Activity

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

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

Privacy and Electronic Communications

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

Use of Cloud Services

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

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

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

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

Where is the cloud?

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



ysgol ardudwy

Security concerns

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

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

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

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

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

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

The Online Safety Resource available from Hwb has a variety of strands, one of which focuses on Privacy and Security. There are opportunities to learn strategies for managing online information and keeping it secure online risks such as identity thieves and phishing. Learners learn how to create strong passwords, how to avoid scams and schemes, and how to analyse privacy policies.

Monitoring users

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

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

With all of those separate user folders and portfolios with their separate passwords and widely varying content, how can you be sure they are not being used to store inappropriate materials? Illegal materials? The School provides the tools, e.g. Office 365 and there is therefore an



ysgol ardudwy

expectation that the School should ensure that users are operating in a space that is safe as can be created.

Microsoft state in their user agreements that they reserve the right to actively search stored files.

This means that the School also needs to be clear about what the expectations are around illegal and inappropriate content and how it intends to ensure those expectations are met. These might include:

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

Managing accounts and users

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

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

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

If things go wrong

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

- clear and well communicated policy
- effective routines for securing and recording evidence
- established reporting routes that are well-communicated, respected and agreed by all
- clearly communicated sanctions that have been agreed and shared with all users
- audit trails that are used to shape interventions and inform future practice



ysgol ardudwy

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

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

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

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

B3 School Mobile Technologies Policy Template (inc. BYOD/BYOT)

Mobile technology devices may be a School owned/provided or privately owned 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.

The absolute key to considering the use of mobile technologies is that the learners, staff and wider school community understand that the primary purpose of having their personal device at school is educational and that this is irrespective of whether the device is School owned/provided or personally owned. The mobile technologies policy should sit alongside a range of policies including but not limited to the safeguarding policy, anti-bullying policy, acceptable use agreement, policies around theft or malicious damage and the behaviour policy. Teaching about the safe and appropriate use of mobile technologies should be included in the online safety education programme.

A policy that completely prohibits pupil/student, staff or visitors from bringing mobile technologies to the school/academy could be considered to be unreasonable and unrealistic for school/academy to achieve. For example many parents/carers would also be concerned for health and safety reasons if their child were not allowed to carry a mobile phone and many staff and visitors use



ysgol ardudwy

mobile phones to stay in touch with family. Contractors require mobile technologies for legitimate business reasons.

Potential Benefits of Mobile Technologies

Research has highlighted the widespread uptake of mobile technologies amongst adults and children of all ages. Web-based tools and resources have changed the landscape of learning. Learners now have at their fingertips unlimited access to digital content, resources, experts, databases and communities of interest. By effectively maximizing the use of such resources, schools not only have the opportunity to deepen learning, but they can also develop digital literacy, fluency and citizenship in learners that will prepare them for the high-tech world in which they will live, learn and work.

For further reading, please refer to "Bring your own device: a guide for schools" by Alberta Education available at: <http://education.alberta.ca/admin/technology/research.aspx> and to the " NEN Technical Strategy Guidance Note 5 – Bring your own device" - <http://www.nen.gov.uk/bring-your-own-device-byod/>

Considerations

There are a number of issues and risks to consider when implementing mobile technologies, these include; security risks in allowing connections to your School network, filtering of personal devices, breakages and insurance, access to devices for all learners, avoiding potential classroom distraction, network connection speeds, types of devices, charging facilities, total cost of ownership

Schools/colleges may consider implementing the use of mobile technologies as a means of reducing expenditure on school provided devices. However, it is important to remember that the increased network management costs and overheads involved in implementing this properly are likely to counterbalance or outweigh any savings.

The use of mobile technologies brings both real benefits and challenges for the whole school community – including teachers - and the only effective way for a school to implement these successfully is to involve the whole school community from the outset. Before the school embarks on this path, the risks and benefits must be clearly identified and shared with all stakeholders.

- **The School has addressed broadband performance and capacity to ensure that core educational and administrative activities are not negatively affected by the increase in the number of connected devices**
- **The School has provided technical solutions for the safe use of mobile technology for School devices and for personal devices**
- **For all mobile technologies, filtering will be applied to the School internet connection and attempts to bypass this are not permitted**
- **Where mobile broadband (e.g. 3G and 4G) use is allowed in the school /college, users are required to follow the same acceptable use requirements as they would if using School owned devices.**
- **Mobile technologies must only be used in accordance with the law**
- **Mobile technologies are not permitted to be used in certain areas within the School site such as changing rooms, toilets and swimming pools.**



ysgol ardudwy

- **Learners will be educated in the safe and appropriate use of mobile technologies as part of the online safety curriculum**
- The school acceptable use agreements for staff, learners, parents and carers will give consideration to the use of mobile technologies
- The school allows:

	School Devices			Personal Devices		
	School and allocated to a single user	School owned for use by multiple users	Authorised device ⁶	Pupil/Student owned	Staff owned	Visitor owned
Allowed in school/college	Yes	Yes	Yes	No	Yes	Yes
Full network access	Yes	Yes	Yes	No	Yes	Yes
Internet only				No		
No network access						

School devices

- **All School devices are controlled through the use of mobile device management (MDM) software**
- **Appropriate access control is applied to all mobile devices according to the requirements of the user (e.g internet only access, network access allowed, shared folder network access)**
- **All School devices must be suitably protected via a passcode/password/pin (and encryption where relevant). Those devices allocated to members of staff must only be accessed and used by members of staff**
- **Appropriate exit processes are implemented for devices no longer used at a School location or by an authorised user.**
- **The software / apps originally installed by the School must remain on the School owned device in usable condition and be easily accessible at all times. From time to time the School may add software applications for use in a**

⁶ 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



ysgol ardudwy

particular lesson. Periodic checks of devices will be made to ensure that users have not removed required apps

- **The School will ensure that School devices contain the necessary apps for Schoolwork. Apps added by the School will remain their property and will not be accessible to learners on authorised devices once they leave the School roll. Any apps bought by the user on their own account will remain theirs**
- **The School is responsible for keeping devices up to date through software, security and app updates. The device is virus protected and should not be capable of passing on infections to the network. Where user intervention or support for this process is required, this will be made clear to the user**
- **School devices are provided to support learning. It is expected that learners will bring devices to school as required**
- **The changing of settings (exceptions include personal settings such as font size, brightness, etc.) that would stop the device working as it was originally set up and intended is not permitted**
- *All school devices are subject to routine monitoring*
- *Pro-active monitoring has been implemented to monitor activity*

Personal devices

When personal devices are permitted:

- *All personal devices are restricted through the implementation of technical solutions that provide appropriate levels of filtered network access*
- *Personal devices are brought into the School entirely at the risk of the owner and the decision to bring the device in to the School lies with the user (and their parents/carers) as does the liability for any loss or damage resulting from the use of the device in the school/college*
- *Staff personal devices should not be used to contact learners or their families, nor should they be used to take images of learners*



ysgol ardudwy

- *The School accepts no responsibility or liability in respect of lost, stolen or damaged devices while at the School or on activities organised or undertaken by the School (the School recommends insurance is purchased to cover that device whilst out of the home)*
- *The School accepts no responsibility for any malfunction of a device due to changes made to the device while on the School network or whilst resolving any connectivity issues*
- *The School recommends that the devices are made easily identifiable and have a protective case to help secure them as the devices are moved around the school. Pass-codes or PINs should be set on personal devices to aid security*
- *The School is not responsible for the day to day maintenance or upkeep of the user's personal device such as the charging of any device, the installation of software updates or the resolution of hardware issues*
- *Personal devices should be charged before being brought to the School as the charging of personal devices is not permitted during the school day*

User behaviour

Users are expected to act responsibly, safely and respectfully in line with current acceptable use agreements, in addition;

- **The sending of abusive or inappropriate messages or content via mobile phones or personal devices is forbidden by any member of the community and any breaches will be dealt with as part of the discipline/behaviour policy**
- **Guidance is made available by the School to users concerning where and when mobile devices may be used**
- **Devices may not be used in tests or exams**
- **Users are responsible for keeping their device up to date through software, security and app updates. The device is virus protected and should not be capable of passing on infections to the network**
- **Users are responsible for charging their own devices and for protecting and looking after their devices while in the school/college**
- **Devices must be in silent mode on the School site and on School buses**
- **Users should be mindful of the age limits for app purchases and use and should ensure they read the terms and conditions before use.**
- **Learners must only photograph people with their permission and must only take pictures or videos that are required for a task or activity. All unnecessary images or videos will be deleted immediately**
- *Devices may be used in lessons in accordance with teacher direction*
- *Staff owned devices should not be used for personal purposes during teaching sessions, except in emergency situations*
- *Printing from personal devices will not be possible*



ysgol ardudwy

B4 Social Media Template Policy

Social media (e.g. Facebook, Twitter, LinkedIn) is a broad term for any kind of online platform which enables people to directly interact with each other. However some games, for example Minecraft or World of Warcraft and video sharing platforms such as You Tube have social media elements to them.

The School recognises the numerous benefits and opportunities which a social media presence offers. Staff, parents and carers and learners are actively encouraged to find creative ways to use social media. However, there are some risks associated with social media use, especially around the issues of safeguarding, bullying and personal reputation. This policy aims to encourage the safe use of social media by the School its staff, parents and carers and learners.



ysgol ardudwy

Scope

This policy is subject to the school's codes of conduct and acceptable use agreements.

This policy:

- applies to all staff and to all online communications which directly or indirectly, represent the school.
- applies to such online communications posted at any time and from anywhere.
- encourages the safe and responsible use of social media through training and education
- *defines the monitoring of public social media activity pertaining to the school*

The School respects privacy and understands that staff and learners may use social media forums in their private lives. However, personal communications likely to have a negative impact on professional standards and/or the school's reputation are within the scope of this policy.

Professional communications are those made through official channels, posted on a School account or using the school name. All professional communications are within the scope of this policy.

Personal communications are those made via a personal social media accounts. In all cases, where a personal account is used which associates itself with, or impacts on the school/college, it must be made clear that the member of staff is not communicating on behalf of the School 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.

Digital communications with learners are also considered. Staff may use social media to communicate with learners via a school social media account for teaching and learning purposes but must consider whether this is appropriate and consider the potential implications.

Organisational control

Roles & Responsibilities

- SLT
 - facilitating training and guidance on Social Media use.
 - developing and implementing the Social Media policy
 - taking a lead role in investigating any reported incidents.
 - making an initial assessment when an incident is reported and involving appropriate staff and external agencies as required.
 - receive completed applications for Social Media accounts
 - approve account creation
- Administrator / Moderator
 - create the account following SLT approval
 - store account details, including passwords securely
 - be involved in monitoring and contributing to the account
 - control the process for managing an account after the lead staff member has left the School(closing or transferring)
- Staff
 - know the contents of and ensure that any use of social media is carried out in line with this and other relevant policies



ysgol ardudwy

- attending appropriate training
- regularly monitoring, updating and managing content he/she has posted via school accounts
- adding an appropriate disclaimer to personal accounts when naming the school/college

Managing accounts

- Process for creating new accounts

The School community is encouraged to consider if a social media account will help them in their work, eg a history department Twitter account, or a "Friends of the school/college" Facebook page. Anyone wishing to create such an account must present a business case to the School Leadership Team which covers the following points: -

- the aim of the account
- the intended audience
- how the account will be promoted
- who will run the account (at least two staff members should be named)
- will the account be open or private/closed

Following consideration by the SLT an application will be approved or rejected. In all cases, the SLT must be satisfied that anyone running a social media account on behalf of the School has read and understood this policy and received appropriate training. This also applies to anyone who is not directly employed by the school/college, including volunteers or parents.

Monitoring

- **School accounts must be monitored regularly and frequently** (preferably 7 days a week, including during holidays). Any comments, queries or complaints made through those accounts must be responded to within 24 hours (or on the next working day if received at a weekend) even if the response is only to acknowledge receipt. Regular monitoring and intervention is essential in case a situation arises where bullying or any other inappropriate behaviour arises on a school social media account.

Behaviour

- **The School requires that all users using social media adhere to the standard of behaviour as set out in this policy and other relevant policies.**
- **Digital communications by staff must be professional and respectful at all times and in accordance with this policy.** Staff will not use social media to infringe on the rights and privacy of others or make ill-considered comments or judgments about staff. School social media accounts must not be used for personal gain. Staff must ensure that confidentiality is maintained on social media even after they leave the employment of the school.
- Users must declare who they are in social media posts or accounts. Anonymous posts are discouraged in relation to School activity.
- If a journalist makes contact about posts made using social media staff must follow the School media policy before responding.
- Unacceptable conduct, (e.g. defamatory, discriminatory, offensive, harassing content or a breach of data protection, confidentiality, copyright) will be considered extremely seriously by the School and will be reported as soon as possible to a relevant senior member of staff, and escalated where appropriate.
- The use of social media by staff while at work may be monitored, in line with School policies. *The School permits reasonable and appropriate access to private social media*



ysgol ardudwy

sites. However, where excessive use is suspected, and considered to be interfering with relevant duties, disciplinary action may be taken

- The School will take appropriate action in the event of breaches of the social media policy. Where conduct is found to be unacceptable, the School will deal with the matter internally. Where conduct is considered illegal, the School will report the matter to the police and other relevant external agencies, and may take action according to the disciplinary policy.

Legal considerations

- Users of social media should consider the copyright of the content they are sharing and, where necessary, should seek permission from the copyright holder before sharing.
- Users must ensure that their use of social media does not infringe upon relevant data protection laws, or breach confidentiality.

Handling abuse

- When acting on behalf of the school/college, handle offensive comments swiftly and with sensitivity.
- If a conversation turns and becomes offensive or unacceptable, School users should block, report or delete other users or their comments/posts and should inform the audience exactly why the action was taken
- If you feel that you or someone else is subject to abuse by colleagues through use of a social networking site, then this action must be reported using the agreed School protocols.

Tone

- The tone of content published on social media should be appropriate to the audience, whilst retaining appropriate levels of professional standards. Key words to consider when composing messages are:
 - engaging
 - conversational
 - informative
- friendly (on certain platforms, eg. Facebook)

Use of images

- School use of images can be assumed to be acceptable, providing the following guidelines are strictly adhered to.
- **permission to use any photos or video recordings should be sought in line with the school's/college's digital and video images policy.** If anyone, for any reason, asks not to be filmed or photographed then their wishes should be respected
- **under no circumstances should staff share or upload learner pictures online other than via School owned social media accounts**
- staff should exercise their professional judgement about whether an image is appropriate to share on School social media accounts. Students should be appropriately dressed, not be subject to ridicule and must not be on any School list of children whose images must not be published
- if a member of staff inadvertently takes a compromising picture which could be misconstrued or misused, they must delete it immediately.



ysgol ardudwy

Personal use

Staff

- personal communications are those made via a personal social media accounts. In all cases, where a personal account is used which associates itself with, or impacts on, the school/college, it must be made clear that the member of staff is not communicating on behalf of the School 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 the 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.*

Pupil/Students

- Staff are not permitted to follow or engage with current or prior learners of the School on any personal social media network account
- the school's/college's education programme should enable the learners to be safe and responsible users of social media
- learners are encouraged to comment or post appropriately about the school. Any offensive or inappropriate comments will be resolved by the use of the school's behaviour policy

Parents/Carers

- If parents/carers have access to a school learning platform where posting or commenting is enabled, parents/carers will be informed about acceptable use
- the School has an active parent and carer education programme which supports the safe and positive use of social media. This includes information on the website
- parents and carers are encouraged to comment or post appropriately about the school/college. In the event of any offensive or inappropriate comments being made, the School will ask the parent/carers to remove the post and invite them to discuss the issues in person. If necessary, refer parents to the school's complaints procedures.

Monitoring posts about the school

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

Appendix

Managing your personal use of Social Media:

- "nothing" on social media is truly private
- social media can blur the lines between your professional and private life. Don't use the school logo and/or branding on personal accounts
- check your settings regularly and test your privacy
- keep an eye on your digital footprint
- keep your personal information private
- regularly review your connections – keep them to those you want to be connected to
- when posting online consider; Scale, Audience and Permanency of what you post
- if you want to criticise, do it politely



ysgol ardudwy

- take control of your images – do you want to be tagged in an image? What would children or parents say about you if they could see your images?
- know how to report a problem

Managing school social media accounts

The Do's

- Check with a senior leader before publishing content that may have controversial implications for the school
- use a disclaimer when expressing personal views
- make it clear who is posting content
- use an appropriate and professional tone
- be respectful to all parties
- ensure you have permission to 'share' other peoples' materials and acknowledge the author
- express opinions but do so in a balanced and measured manner
- think before responding to comments and, when in doubt, get a second opinion
- seek advice and report any mistakes using the school's reporting process
- consider turning off tagging people in images where possible

The Don'ts

- Don't make comments, post content or link to materials that will bring the school into disrepute
- don't publish confidential or commercially sensitive material
- don't breach copyright, data protection or other relevant legislation
- consider the appropriateness of content for any audience of school accounts, and don't link to, embed or add potentially inappropriate content
- don't post derogatory, defamatory, offensive, harassing or discriminatory content
- don't use social media to air internal grievances



ysgol ardudwy

B5 Schoolpolicy template - Online safety group terms of reference

1. PURPOSE

To provide a consultative group that has wide representation from the School community, with responsibility for issues regarding online safety and the monitoring the online safety policy including the impact of initiatives.

2. MEMBERSHIP

2.1 The online safety group will seek to include representation from all stakeholders.

The composition of the group should include (n.b. in small schools/colleges one member of staff may hold more than one of these posts): [add/delete where appropriate]

- SLT member/s
- safeguarding officer
- teaching staff member
- support staff member
- online safety co-ordinator (not ICT coordinator by default)
- governor
- parent/carer
- technical support staff (where possible)
- community users (where appropriate)
- *learner representation* – for advice and feedback. *Learner voice is essential in the make up of the online safety group, but learners would only be expected to take part in meetings where deemed relevant.*

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

2.3 Group members must declare a conflict of interest if any incidents being discussed directly involve

themselves or members of their families.

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

confidential nature

2.5 When individual members feel uncomfortable about what is being discussed they should be allowed to leave

the meeting with steps being made by the other members to allow for these sensitivities

3. CHAIRPERSON

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

- scheduling meetings and notifying group members;
- inviting other people to attend meetings when required by the group;



ysgol ardudwy

- guiding the meeting according to the agenda and time available;
- ensuring all discussion items end with a decision, action or definite outcome;
- making sure that notes are taken at the meetings and that these with any action points are distributed as necessary

4. DURATION OF MEETINGS

Meetings shall be held **each term** for a period of **1** hour(s). A special or extraordinary meeting may be called when and if deemed necessary.

5. FUNCTIONS

These are to assist the online safety co-ordinator (or other relevant person) with the following:

- to keep up to date with new developments in the area of online safety
- to (at least) annually review and develop the online safety policy in line with new technologies and incidents
- to monitor the delivery and impact of the online safety policy
- to monitor the log of reported online safety incidents (anonymous) to inform future areas of teaching/learning/training.
- to co-ordinate consultation with the whole School community to ensure stakeholders are up to date with information, training and/or developments in the area of online safety. This could be carried out through
 - staff meetings
 - learner forums (for advice and feedback)
 - governors meetings
 - surveys/questionnaires for learners, parents/carers and staff
 - parents evenings
 - website/learning platform/newsletters
 - online safety events
 - Internet Safety Day (annually held on the second Tuesday in February)
 - other methods
- to ensure that monitoring is carried out of Internet sites used across the School(if possible)
- to monitor filtering/change control logs (e.g. requests for blocking/unblocking sites).
- to monitor the safe use of data across the school
- to monitor incidents involving cyberbullying for staff and pupils

6. AMENDMENTS

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

The above Terms of Reference for **[insert name of organisation]** have been agreed

Signed by (SLT):

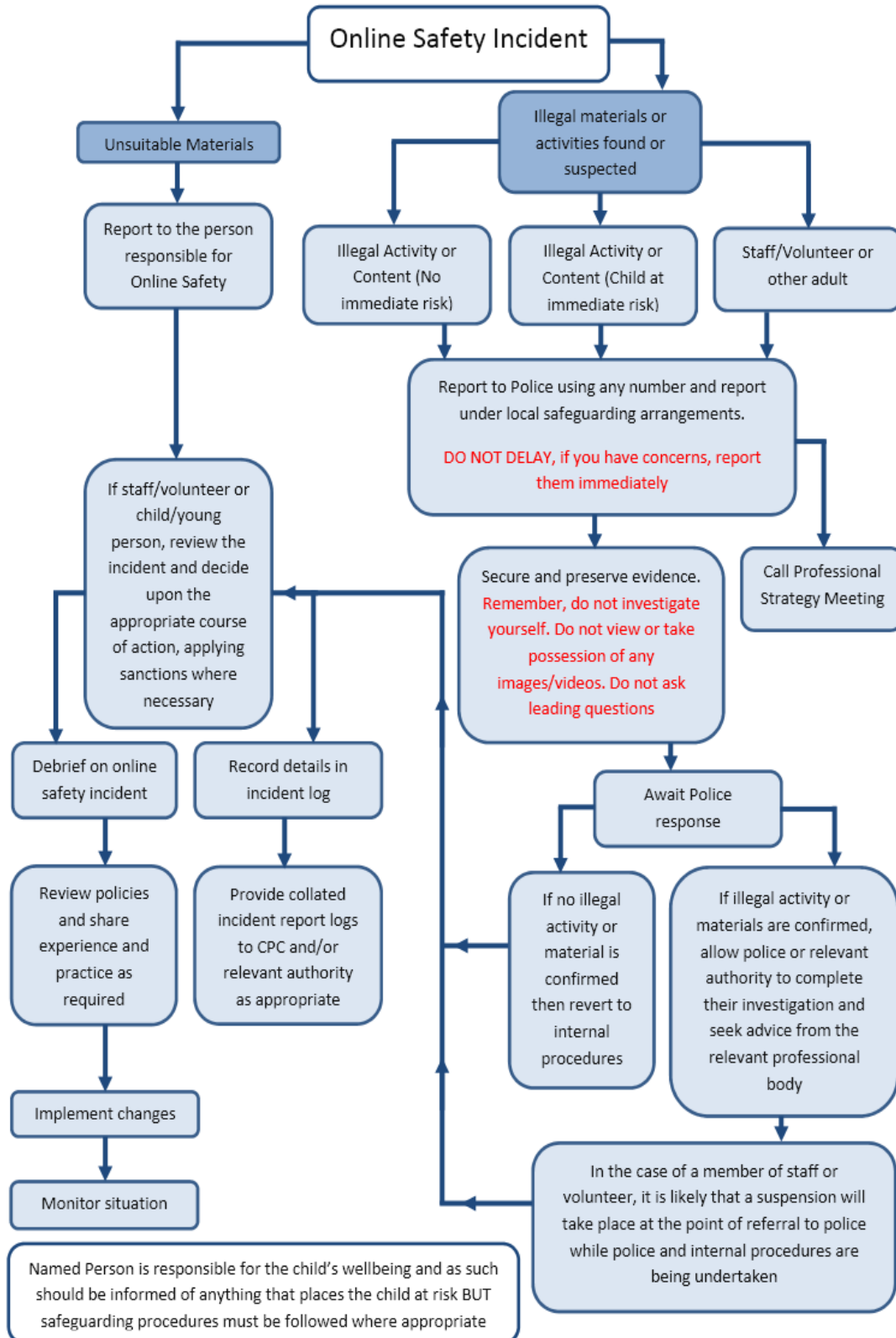
Date:

Date for review:



ysgol arduwy

Acknowledgement C1 Responding to incidents of misuse – flow chart





ysgol ardudwy

C2 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
----------------------------	--------------------

Web site(s) address/device	Reason for concern

Conclusion and action proposed or taken

C3 Reporting Log Template

Group:

Date	Time	Incident	Action Taken		Incident Reported By	Signature
			What?	By Whom?		

C4 Training Needs Audit Log Template

Group:

Relevant training the last 12 months	Identified Training Need	To be met by	Cost	Review Date		

C5 Summary of Legislation

Schools/colleges 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.

Data Protection Act 1998

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

- fairly and lawfully processed.
- processed for limited purposes.
- adequate, relevant and not excessive.
- accurate.
- not kept longer than necessary.
- processed in accordance with the data subject's rights.
- secure.
- not transferred to other countries without adequate protection.

Freedom of Information Act 2000

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

Communications Act 2003

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

Malicious Communications Act 1988

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

Regulation of Investigatory Powers Act 2000

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

- establish the facts;
- ascertain compliance with regulatory or self-regulatory practices or procedures;
- demonstrate standards, which are or ought to be achieved by persons using the system;
- investigate or detect unauthorised use of the communications system;
- prevent or detect crime or in the interests of national security;
- ensure the effective operation of the system.
- monitoring but not recording is also permissible in order to:
 - ascertain whether the communication is business or personal;
 - protect or support help line staff

Trade Marks Act 1994

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

Copyright, Designs and Patents Act 1988

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

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

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

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

Racial and Religious Hatred Act 2006/Public Order Act 1986

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

Protection from Harassment Act 1997

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

Protection of Children Act 1978

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

Sexual Offences Act 2003

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, connections staff fall in this category of trust). Any sexual intercourse with a child under the age of 13 commits the offence of rape.

Public Order Act 1986

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

Obscene Publications Act 1959 and 1964

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

Human Rights Act 1998

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

- the right to a fair trial

- the right to respect for private and family life, home and correspondence
- freedom of thought, conscience and religion
- freedom of expression
- freedom of assembly
- prohibition of discrimination
- the right to education
- the right not to be subjected to inhuman or degrading treatment or punishment

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

The Protection of Freedoms Act 2012

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

C6 Office 365 – further information

Where is the data stored?

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

How often is the data backed up?

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

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

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

How does the email provider protect your privacy?

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

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

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

Who has access to the data?

By default no one has access to customer data within the Office 365 service. Microsoft employees who have completed appropriate background checks and have justified need

can raise an escalation for time-limited access to Customer data. Access is regularly audited, logged and verified through the ISO 27001 Certification.

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

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

Schools/colleges may wish to consider the extent to which applicable laws in the US – which apply to services operated by companies registered in the US, e.g. Microsoft and Google – affect the suitability of these services. For example the US Patriot Act provides a legal means through which law enforcement agencies can access data held within these services without necessarily needing the consent or even the knowledge of the customer. Whilst SWGfL doesn't intend to put anyone off getting value from these beneficial services we feel it's only right to share what we know about them.

Is personal information shared with anyone else?

No personal information is shared.

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

No. There is no advertising in Office365.

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

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

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

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

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

How reliable is the email service?

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

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

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

Additional Resources

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

C7 Links to other organisations or documents

These may help those who are developing or reviewing an online safety policy.

UK Safer Internet Centre

- [Safer Internet Centre](#)
- [South West Grid for Learning](#)
- [Childnet](#)
- [Professionals Online Safety Helpline](#)
- [Internet Watch Foundation](#)

CEOP

- <http://ceop.police.uk/>
- [ThinkUKnow](#)

Others

- INSAFE - <http://www.saferinternet.org/ww/en/pub/insafe/index.htm>
- UK Council for Child Internet Safety (UKCCIS) - www.education.gov.uk/ukccis
- Netsmartz - <http://www.netsmartz.org/index.aspx>

Cyberbullying

- Scottish Anti-Bullying Service, Respectme - <http://www.respectme.org.uk/>
- Scottish Government - [Better relationships, better learning, better behaviour](#)
- [Welsh Government – Respecting Others](#)
- Anti-Bullying Network - <http://www.antibullying.net/cyberbullying1.htm>
- Cyberbullying.org - <http://www.cyberbullying.org/>
- Enable – EU funded anti-bullying project - <http://enable.eun.org/>

Sexting

- [UKCCIS - Sexting in schools and colleges: responding to incidents and safeguarding young people](#) (to be added to both language versions)
- [UKSIC – Responding to and managing sexting incidents](#)

Social Networking

- Digizen – [Social Networking](#)
- [SWGfL - Facebook - Managing risk for staff and volunteers working with children and young people](#)
- [Connectsafely Parents Guide to Facebook](#)
- [Facebook Guide for Educators](#)

Curriculum

- [SWGfL Online Safety Resource \(accessed through Hwb\)](#)
- Alberta, Canada - [digital citizenship policy development guide.pdf](#)
- Teach Today – www.teachtoday.eu/
- Insafe - [Education Resources](#)

Mobile Devices/BYOD

Cloudlearn Report [Effective practice for schools moving to end locking and blocking](#)

NEN - [Guidance Note - BYOD](#)

Data Protection

- Information Commissioners Office:
 - [Your rights to your information – Resources for Schools - ICO](#)
 - [ICO pages for young people](#)

- [Guide to Data Protection Act - Information Commissioners Office](#)
 - [Guide to the Freedom of Information Act - Information Commissioners Office](#)
 - [ICO - Guidance we gave to schools/colleges - September 2012 \(England\)](#)
 - [ICO Guidance on Bring Your Own Device](#)
 - [ICO Guidance on Cloud Computing](#)
 - [Information Commissioners Office good practice note on taking photos in schools/colleges](#)
 - [ICO Guidance Data Protection Practical Guide to IT Security](#)
 - [ICO – Think Privacy Toolkit](#)
 - [ICO – Personal Information Online – Code of Practice](#)
 - [ICO – Access Aware Toolkit](#)
 - [ICO Subject Access Code of Practice](#)
 - [ICO – Guidance on Data Security Breach Management](#)
- SWGfL - [Guidance for Schools/colleges on Cloud Hosted Services](#)
 - NEN - [Guidance Note - Protecting SchoolData](#)

Professional Standards/Staff Training

- Kent - Safer Practice with Technology
- Childnet/TDA - Social Networking - a guide for trainee teachers & NQTs
- Childnet/TDA - Teachers and Technology - a checklist for trainee teachers & NQTs
- UK Safer Internet Centre Professionals Online safety Helpline

Infrastructure/Technical Support

- Somerset - [Questions for Technical Support](#)
- NEN - [Guidance Note - esecurity](#)

Working with parents and carers

- [Connect Safely - a Parents Guide to Facebook](#)
- [Vodafone Digital Parents Magazine](#)
- [Childnet Webpages for Parents & Carers](#)
- [Get Safe Online - resources for parents](#)
- [Teach Today - resources for parents workshops/education](#)
- The Digital Universe of Your Children - animated videos for parents (Insafe)
- Cerebra - Learning Disabilities, Autism and Internet Safety - a Parents' Guide
- Insafe - A guide for parents - education and the new media
- [Internetmatters.org](#)

Research

- [EU Kids on Line Report - "Risks and Safety on the Internet" - January 2011](#)
- [Futurelab - "Digital participation - its not chalk and talk any more!"](#)

C8 Glossary of terms

AUA	Acceptable use agreement – 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
FOSI	Family Online safety Institute
EA	Education Authority
ICO	Information Commissioners Office
ICT	Information and Communications Technology
ICTMark	Quality standard for schools/colleges 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 (e.g. SWGfL) to provide the safe broadband provision to schools/colleges across Britain.
Ofcom	Office of Communications (Independent communications sector regulator)
SWGfL	South West Grid for Learning Trust – the Regional Broadband Consortium of SW Local Authorities – is the provider of broadband and other services for schools/colleges and other organisations in the SW
TUK	Think U Know – educational Online safety programmes for schools/colleges, 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

Copyright of the SWGfL School Online safety policy Templates is held by SWGfL. Schools/colleges and other educational institutions are permitted free use of the templates. Any person or organisation wishing to use the document for other purposes should seek consent from SWGfL and acknowledge its use.

Every reasonable effort has been made to ensure that the information included in this template is accurate, as at the date of publication in October 2014. However, SWGfL cannot guarantee its accuracy, nor can it accept liability in respect of the use of the material whether in whole or in part and whether modified or not. Suitable legal/professional advice should be sought if any difficulty arises in respect of any aspect of this new legislation or generally to do with School conduct or discipline.

ⁱ In a small school/college some of the roles described below may be combined, though it is important to ensure that there is sufficient “separation of responsibility” this the cas.

ⁱⁱ It is suggested that the role may be combined with that of the Safeguarding Governor