YSGOL BRO GWAUN

ONLINE SAFETY AND THE USE OF DIGITAL TECHNOLOGIES

DIOGELWCH AR-LEIN A DEFNYDDIO'R TECHNOLEGAU DIGIDOL

Adolygiad/Review: Blynyddol / Annually

Adolygiad nesaf/Next Review: <date>

Wedi Cytuno gan Bwyllgor y Llywodraethwyr

Approved by Governors Committee

Arwyddwyd/Signed:

Pennaeth/Headteacher: ____

Llywodraethwr/Governor: ____

Rhiant/Parent: ____

ONLINE SAFETY AND THE USE OF DIGITAL TECHNOLOGIES
DIOGELWCH AR-LEIN A DEFNYDDIO POLISI TECHNOLEGAU DIGIDOL

Rheoli Dogfennau / Document Control:

Fersiwn/ Version	**Adolygiad/ Reviewed**	**Crynodeb o Newidiadau / Summary of changes**	**Wedi cytuno / Approved:**
1.0		Original document	

Mae copi cyflawn o'r polisi hwn ar gael o swyddfa'r ysgol ar gais, gyda dyddiad cymmeradwyaeth, dyddiad adolygu a llofnod bob rhanddeiliad oedd yn rhan o cymmeradwyaeth polisi.

A complete copy of this policy is available from the school office upon request, they include an approval date, a review date and signatures of all stakeholders involved in the approval of the policy.

Contents

Development/Monitoring/Review of this Policy

This online safety policy has been developed by a working group/committee Ysgol Bro Gwaun's Online Safety working group made up of:

- Headteacher and senior leaders
- Online Safety Officer
- Staff – including teachers, support staff, technical staff
- Governors/Board
- Parents and carers
- Digital Leaders
- School Council

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

Schedule for Development/Monitoring/Review

This online safety policy was approved by the Board of Governing Body on:	*2020*
The implementation of this online safety policy will be monitored by the:	Online Safety Working Group
Monitoring will take place at regular intervals:	Annually
The Governing Body 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:	Annually, unless a significant event occurs
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:	Annually
Should serious online safety incidents take place, the following external persons/agencies should be informed:	Within School – Designated CPO/Headteacher

The school will monitor the impact of the policy using:

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

Scope of the Policy

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

The Education and Inspections Act 2006 empowers Headteachers to such extent as is reasonable, to regulate the behaviour of students/pupils when they are off the *school* site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of online-bullying or other online safety incidents covered by this policy, which may take place outside of the *school*, but is linked to membership of the school.

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

Roles and Responsibilities

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

Governors

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

- meetings with the CPO/Online Safety Lead
- monitoring of Online Safety incident logs
- 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 CPO/ICT Lead.
- The Headteacher and (at least) another member of the Senior Leadership Team / Senior Management Team should be aware of the procedures to be followed in the event of a serious Online Safety allegation being made against a member of staff.
- The Headteacher / Senior Leaders are responsible for ensuring that the CPO/ICT Lead and other relevant staff receive suitable training to enable them to carry out their Online Safety roles and to train other colleagues, as relevant.
- The Headteacher / Senior Leaders will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal Online Safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.
- The Senior Leadership Team will receive monitoring reports from the ICT Lead/CPO whenever incidents occur or if changes to the policy/infrastructure are made.

Online Safety Lead

- leads the Online Safety committee
- 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) technical staff
- receives reports of Online Safety incidents 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 Senior Leadership Team

Network Manager/Technical staff

The Network Manager / Technical Staff (or managed service provider) is responsible for ensuring:

- that the school's technical infrastructure is secure and is not open to misuse or malicious attack
- that the school meets (as a minimum) the required 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 the filtering policy (Smoothwall), is applied and updated on a regular basis and its implementation is not the sole responsibility of any single person
- that they keep up to date with 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 / Virtual Learning Environment / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the Headteacher / Senior Leader; ICT Lead/CPO for investigation / action / sanction
- that screen monitoring software (Veyon) is implemented and updated as agreed in school policies
- that monitoring and filtering software (Securus and Smoothwall) is set up as per the policy and training needs are met for staff using the tools.

Teaching and Support Staff

Are responsible for ensuring that:

- they have an up to date awareness of Online Safety matters and of the current school Online Safety policy and practices
- they have read, understood and signed the Staff Acceptable Use Policy / Agreement (AUP / AUA)
- they report any suspected misuse or problem to the Headteacher / Senior Leader; CPO/ICT Lead for investigation / action
- all digital communications with students / pupils / parents / carers should be on a professional level and only carried out using official school systems (Email, Xpressions, Microsoft Teams, Google Classroom/Meet)
- Online Safety issues are embedded in all aspects of the curriculum and other activities
- students / pupils understand and follow the Online Safety and acceptable use agreements / policies
- students / pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- they monitor the use of digital technologies, mobile devices, cameras etc in lessons and other school activities (where allowed) and implement current policies with regard to these devices
- in lessons where internet use is pre-planned students / pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches

Designated Safeguarding Lead/Designated Person/Officer

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

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

Online Safety Group

The Online Safety Group provides a consultative group that has 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. 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 Lead (or other relevant person, as above) with:

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

Students/Pupils:

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

Parents/carers

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

- digital and video images taken at school events
- access to parents' sections of the website/Learning Platform and on-line student/pupil records (classcharts)

Policy Statements

Education – Students/Pupils

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

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

- A planned online safety curriculum should be provided as part of Digital Technology/Health and Wellbeing/PSHE lessons and should be regularly revisited
- Key online safety messages should be reinforced as part of a planned programme of assemblies and tutorial/pastoral activities (use of Police Liaison Officer)
- Students/pupils should be taught in all lessons to be critically aware of the materials/content they access on-line and be guided to validate the accuracy of information.
- Students/pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Students/pupils 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 (Prevent Strategy).
- *Students/pupils should be helped to understand the need for the student/pupil acceptable use agreement and encouraged to adopt safe and responsible use both within and outside school.*
- *Staff should act as good role models in their use of digital technologies, the internet and mobile devices*
- *Where students/pupils 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 relevant designated 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.*
- *Targeted invention will take place following a survey to gather pupils' prior knowledge of digital resilience before targeted lessons will take place. Following the teaching of set topics, pupils will be re-surveyed to identify the impact of the intervention.*

Education – Parents/carers

Many parents and carers have only a limited understanding of online safety risks and issues, yet they play an essential role in the education of their children and in the monitoring/regulation of the children's online behaviours. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.

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

- *Curriculum activities*
- *Letters, newsletters, web site, Learning Platform*
- *Parents/carers evenings/sessions*
- *Social Media*
- *High profile events/campaigns e.g. Safer Internet Day*
- *Reference to the relevant web sites/publications such as the HWB online Safety area.*

Education – The Wider Community

The school will provide opportunities for local community groups/members of the community to gain from the schools' 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 (Springboard and LA)*
- *The school website will provide online safety information for the wider community*
- *Sharing their online safety expertise/good practice with other local schools*
- *Supporting community groups*

Education & Training – Staff/Volunteers

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

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

Training – Governors/Directors

Governors/Directors should take part in online safety training/awareness sessions, with particular importance for those who are members of any 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/MAT/National Governors Association/or other relevant organisation (e.g. SWGfL).
- Participation in school training/information sessions for staff or parents (this may include attendance at assemblies/lessons).

Technical – infrastructure/equipment, filtering and monitoring

The school will be responsible for ensuring that the school infrastructure/network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also need to ensure that the relevant people named in the above sections will be effective in carrying out their 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 school technical systems and devices.
- All users will be provided with a username and secure password by the Network Manager *who will keep an up to date record of users and their usernames.* Users are responsible for the security of their username and password.

- The "master/administrator" passwords for the school 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. school safe)
- Network Manager is responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations
- Internet access is filtered for all users. Illegal content (child sexual abuse images) is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list. Content lists are regularly updated and internet use is logged and regularly monitored. There is a clear process in place to deal with requests for filtering changes
- Internet filtering/monitoring should ensure that children are safe from terrorist and extremist material when accessing the internet.
- *The school has provided enhanced/differentiated user-level filtering*
- *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* (it helpdesk) *for users to report any actual/potential technical incident/security breach to the relevant person, as agreed).*
- Appropriate security measures are in place (schools/academies may wish to provide more detail) to protect the servers, firewalls, routers, wireless systems, work stations, mobile devices, etc. from accidental or malicious attempts which might threaten the security of the school systems and data. These are tested regularly. The school infrastructure and individual devices are protected by up to date virus software.
- A policy is in place for the provision of temporary access of "guests" (trainee teachers, supply teachers (managed by WD)) onto the school systems.
- *An agreed policy (ICT equipment loan scheme) is in place regarding the extent of personal use that users (staff/students) are allowed on school devices that may be used out of school for school purposes.*
- *A PCC training POD is mandatory for all staff in training them on GDPR which includes the use and storage of personal data.*

Mobile Technologies (including BYOD/BYOT)

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

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

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

	School Devices			Personal Devices		
	School owned for single user	School owned for multiple users	Authorised device	Student owned	Staff owned	Visitor owned
Allowed in school	*Yes*	*Yes*	*Yes*	*No*	*Yes*	*Yes*

Full network access	*Yes*	*Yes*				
Internet only			*Yes*		*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 school/out of school*
- *If personal use is allowed*
- *Levels of access to networks/internet (as above)*
- *Management of devices/installation of apps/changing of settings/monitoring (Meraki and Group Policy)*
- *Network/broadband capacity*
- *Technical support*
- *Filtering of devices*
- *Access to cloud services*
- *Data Protection*
- *Taking/storage/use of images*
- *Exit processes – what happens to devices/software/apps/stored data if user leaves the school*
- *Liability for damage*
- *Staff training*

Personal devices:

- Which users are allowed to use personal mobile devices in school (staff/ visitors)
- Restrictions on where, when and how they may be used in school
- Storage
- Whether staff will be allowed to use personal devices for school business
- Levels of access to networks/internet (as above)
- Network/broadband capacity
- Technical support (this may be a clear statement that no technical support is available)
- Filtering of the internet connection to these devices
- Data Protection
- 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 students/pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents/carers and students/pupils need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for online-bullying to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. It is common for employers to carry out internet searches for information about potential and existing employees. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- When using digital images, staff should inform and educate students/pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.
- Written permission from parents or carers will be obtained before photographs of students/pupils are published on the school website/social media/local press (updated annually through GDPR)
- 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 in not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published/made publicly available on social networking sites, nor should parents/carers comment on any activities involving other *students/pupils* in the digital/video images. Including any events taking part in the school such as Performances and Plays.
- 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 students/pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Students/pupils must not take, use, share, publish or distribute images of others without their permission
- Photographs published on the website, or elsewhere that include students/pupils will be selected carefully and will comply with good practice guidance on the use of such images, in line with the schools 'Use of School's media platforms' policy.
- Students'/Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs.
- Student's/Pupil's work can only be published with the permission of the student/pupil and parents or carers (obtained through annual data return).
- The Safe use of Social Media policy outlines how staff should use social media when posting information on school social platforms.

Data Protection

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

The school must ensure that:

- it has a Data Protection Policy. (see appendix for LA policy)
- it implements the data protection principles and is able to demonstrate that it does so through use of policies, notices and records.
- it has paid the appropriate fee Information Commissioner's Office (ICO) and included details of the Data Protection Officer (DPO).
- it has appointed an appropriate Data Protection Officer (DPO) who has a high level of understanding of data protection law and is free from any conflict of interest. The school has appointed a Data Manager and DPLO (Data protection liaison officer).
- all staff receive data protection training at induction and appropriate refresher training thereafter. Staff undertaking particular data protection functions, such as handling requests under the individual's rights, will receive training appropriate for their function as well as the core training provided to all staff.

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

- data must be encrypted and password protected.
- device must be password protected.

- device must be protected by up to date virus and malware checking software
- data must be securely deleted from the device, in line with school policy once it has been transferred or its use is complete.

Staff must ensure that they:

- at all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse
- can recognise a possible breach, understand the need for urgency and know who to report it to within the school
- can help data subjects understands their rights and know how to handle a request whether verbal or written. Know who to pass it to in the school
- where personal data is stored or transferred on mobile or other devices (including USBs) these must be encrypted and password protected.
- access personal data sources and records only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data

Communications

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

	Staff & other adults				Students/Pupils			
Communication Technologies	Allowed	Allowed at certain	Allowed for	Not allowe	Allowed	Allowed at certain	Allowed with	Not allowe
Mobile phones may be brought to the school	x						x	
Use of mobile phones in lessons				x				x
Use of mobile phones in social time		x						x
Taking photos on personal mobile phones/cameras				x				x
Taking photos on school mobile phones/cameras		x						x
Use of other mobile devices e.g. tablets, gaming devices		x						x
Use of personal email addresses in school, or on school network		x				x		
Use of school email for personal emails				x				x
Use of messaging apps		x						x
Use of social media		x						x

Use of blogs		x					x	

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 students/pupils should therefore use only the school email service to communicate with others when in school, or on school systems (e.g. by remote access).*
- Users must immediately report, to the nominated person – in accordance with the school policy, the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.
- Any digital communication between staff and students/pupils or parents/carers (email, social media, chat, blogs, VLE etc) must be professional in tone and content. *These communications may only take place on official (monitored) school systems. Personal email addresses, text messaging or social media must not be used for these communications.*
- *Students/pupils 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 - Protecting Professional Identity

All schools, academies, MATs and local authorities have a duty of care to provide a safe learning environment for pupils and staff. Schools/academies, MATs and local authorities could be held responsible, indirectly for acts of their employees in the course of their employment. Staff members who harass, engage in online bullying, discriminate on the grounds of sex, race or disability or who defame a third party may render the *school* or local authority/MAT liable to the injured party. Reasonable steps to prevent predictable harm must be in place.

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

- 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 students/pupils, parents/carers or school staff
- They do not engage in online discussion on personal matters relating to members of the school community
- Personal opinions should not be attributed to the *school* or local authority/MAT
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information
- Appendix L highlights 10 top tips from the SWGFL on how to stay safe when using social media: https://hwb.gov.wales/zones/keeping-safe-online/resources/a-teacher-s-guide-to-staying-safe-on-social-media#:~:text=Use%20the%20privacy%20settings,will%20help%20you%20with%20this
- They read and understand the social media checklists in Appendix M on how to lock down accounts and stay safe.

Personal Use:

- Personal communications are those made via a personal social media account. In all cases, where a personal account is used which associates itself with the school or impacts on the school/ academy, 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

Dealing with unsuitable/inappropriate activities

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

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 outside the school when using school equipment or systems. The school policy restricts usage as follows:

User Actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	Child sexual abuse images –The making, production or distribution of indecent images of children. Contrary to The Protection of Children Act 1978 N.B. Schools/academies should refer to guidance about dealing with self-generated images/sexting – UKSIC Responding to and managing sexting incidents and UKCIS – Sexting in schools and colleges					X
	Grooming, incitement, arrangement or facilitation of sexual acts against children Contrary to the Sexual Offences Act 2003.					X
	Possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character) Contrary to the Criminal Justice and Immigration Act 2008					X
	Criminally racist material in UK – to stir up religious hatred (or hatred on the grounds of sexual orientation) - contrary to the Public Order Act 1986					X
	Pornography				X	

	Promotion of any kind of discrimination				X	
	threatening behaviour, including promotion of physical violence or mental harm				X	
	Promotion of extremism or terrorism				X	
	Any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute				X	
Activities that might be classed as cyber-crime under the Computer Misuse Act: • Gaining unauthorised access to school networks, data and files, through the use of computers/devices • Creating or propagating computer viruses or other harmful files • Revealing or publicising confidential or proprietary information (e.g. financial / personal information, databases, computer / network access codes and passwords) • Disable/Impair/Disrupt network functionality through the use of computers/devices • Using penetration testing equipment (without relevant permission) N.B. Schools/academies will need to decide whether these should be dealt with internally or by the police. Serious or repeat offences should be reported to the police. Under the Cyber-Prevent agenda the National Crime Agency has a remit to prevent young people becoming involved in cyber-crime and harness their activity in positive ways – further information here						X
Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school					X	
Revealing or publicising confidential or proprietary information (e.g. financial/personal information, databases, computer/network access codes and passwords)					X	
Unfair usage (downloading/uploading large files that hinders others in their use of the internet)					X	
Using school systems to run a private business					X	
Infringing copyright					X	
On-line gaming (educational)			X			
On-line gaming (non-educational)					X	
On-line gambling - Staff					X	
On-line gambling - Pupils						X
On-line shopping/commerce			X			
File sharing			X			
Use of social media			X			

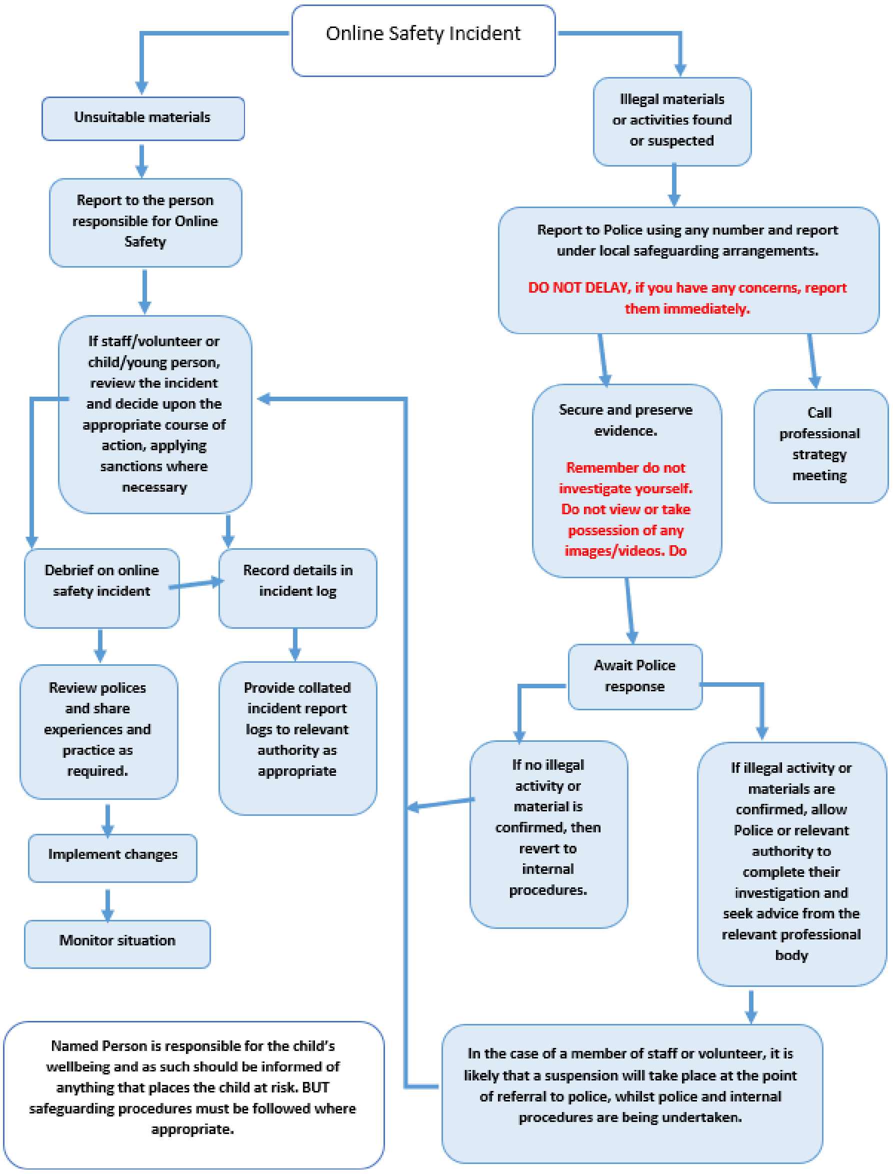
Use of messaging apps		X			
Use of video broadcasting e.g. YouTube		X			

Responding to incidents of misuse

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

Illegal Incidents

If there is any suspicion that the web site(s) concerned may contain child abuse images, or if there is any other suspected illegal activity, refer to the right-hand side of the Flowchart (below) for responding to online safety incidents and report immediately to the police.


Online Safety Incident
Unsuitable materials
Report to the person responsible for Online Safety
If staff/volunteer or child/young person, review the incident and decide upon the appropriate course of action, applying sanctions where necessary
Debrief on online safety incident
Record details in incident log
Review polices and share experiences and practice as required.
Provide collated incident report logs to relevant authority as appropriate
Implement changes
Monitor situation
Named Person is responsible for the child's wellbeing and as such should be informed of anything that places the child at risk. BUT safeguarding procedures must be followed where appropriate.
Illegal materials or activities found or suspected
Report to Police using any number and report under local safeguarding arrangements.
DO NOT DELAY, if you have any concerns, report them immediately.
Secure and preserve evidence.
Remember do not investigate yourself. Do not view or take possession of any images/videos. Do
Call professional strategy meeting
Await Police response
If no illegal activity or material is confirmed, then revert to internal procedures.
If illegal activity or materials are confirmed, allow Police or relevant authority to complete their investigation and seek advice from the relevant professional body
In the case of a member of staff or volunteer, it is likely that a suspension will take place at the point of referral to police, whilst police and internal procedures are being undertaken.

Other Incidents

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

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

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

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

School actions & sanctions

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

Students/Pupils Incidents	Refer to class teacher/tutor	Refer to Head of Department/Year/other	Refer to Headteacher	Refer to Police	Refer to technical support staff for action re filtering/security etc.	Inform parents/carers	Removal of network/internet access rights	Referral to whole school behaviour system (c)
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	X			X	X	X	X
Unauthorised/inappropriate use of mobile phone/digital camera/other mobile device	X	X			X	X		X
Unauthorised/inappropriate use of social media/ messaging apps/personal email	X	X			X	X		X
Unauthorised downloading or uploading of files	X	X			X	X		X
Allowing others to access school network by sharing username and passwords	X	X	X		X	X	X	X
Attempting to access or accessing the school network, using another student's/pupil's account	X	X	X		X	X	X	X
Attempting to access or accessing the school network, using the account of a member of staff	X	X	X		X	X	X	X
Corrupting or destroying the data of other users	X	X	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	X	X

Continued infringements of the above, following previous warnings or sanctions		X	X			X		X
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school		X	X			X		X
Using proxy sites or other means to subvert the schools' filtering system	X	X	X		X	X	X	X
Accidentally accessing offensive or pornographic material and failing to report the incident	X	X	X		X	X	X	X
Deliberately accessing or trying to access offensive or pornographic material	X	X	X	X	X	X	X	X
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act	X	X	X	X	X	X	X	X

Staff Incidents	Refer to line manager	Refer to Headteacher Principal	Refer to Local Authority/HR	Refer to Police	Refer to Technical Support Staff for action re filtering etc.	Warning	Suspension
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	?	?
Inappropriate personal use of the internet/social media/personal email	X	X			X	?	
Unauthorised downloading or uploading of files	X				X		
Allowing others to access school network by sharing username and passwords or attempting to access or accessing the school network, using another person's account	X	X			X	?	
Careless use of personal data e.g. holding or transferring data in an insecure manner	X	X	X		X	?	
Deliberate actions to breach data protection or network security rules	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	?	?
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature	X	X	X	X	X	?	?
Using personal email/social networking/instant messaging/text messaging to carrying out digital communications with students/pupils	X	X	X	?	X	?	?
Actions which could compromise the staff member’s professional standing	X	X	X		X	?	
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school	X	X	X	?	X	?	?
Using proxy sites or other means to subvert the schools’ filtering system	X	X	X		X	?	?
Accidentally accessing offensive or pornographic material and failing to report the incident	X	X	?	?	X	?	?
Deliberately accessing or trying to access offensive or pornographic material	X	X	X	X	X	?	?
Breaching copyright or licensing regulations	X	X				?	

Appendices

Acknowledgements

SWGfL would like to acknowledge the contribution of a wide range of individuals and organisations whose policies, documents, advice and guidance have contributed to the development of the online safety policy templates and of the 360-degree safe online safety self-review tool.

Every effort has been made to ensure that the information included in this document is accurate, as at the date of publication in January 2020. However, SWGfL cannot guarantee its accuracy, nor can it accept liability in respect of the use of the material.

Appendix A - Student/Pupil Acceptable Use Agreement Template – for older students/pupils

School policy

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

This acceptable use agreement is intended to ensure:

- that young people will be responsible users and stay safe while using the internet and other digital technologies for educational, personal and recreational use.
- that school systems and users are protected from accidental or deliberate misuse that could put the security of the systems and will have good access to digital technologies to enhance their learning and will, in return, expect the *students/pupils* 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 the systems, devices and digital communications.
- I will keep my username and password safe and secure – I will not share it, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may steal it.
- I will be aware of "stranger danger", when I am communicating on-line.
- I will not disclose or share personal information about myself or others when on-line (this could include names, addresses, email addresses, telephone numbers, age, gender, educational details, financial details etc.)
- If I arrange to meet people off-line that I have communicated with on-line, I will do so in a public place and take an adult with me.
- I will immediately report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it on-line.

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

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

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

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

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

- I will only use my own personal devices (mobile phones/USB devices etc.) in school if I have permission. I understand that, if I do use my own devices in the *school*, I will follow the rules set out in this agreement, in the same way as if I was using school equipment.

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

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

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

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

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

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

Student/Pupil Acceptable Use Agreement Form

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

Please complete the sections below to show that you have read, understood and agree to the rules included in the acceptable use agreement. If you do not sign and return this agreement, access will not be granted to school systems.

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

- I use the *school* systems and devices (both in and out of school)
- I use my own devices in the *school* (when allowed) e.g. mobile phones, gaming devices USB 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* e.g. communicating with other members of the school, accessing school email, VLE, website etc.
- **Parents are requested to sign the permission form below to show their support of the school in this important aspect of the school's work.**

Name of Student/Pupil: --

Group/Class: --

Signed: --

Date: --

Parent/Carer: --

Appendix B - Student/Pupil Acceptable Use Policy Agreement Template – for younger pupils (Harbwr)

This is how we stay safe when we use computers:

- I will ask a teacher or suitable adult if I want to use the computers/tablets
- I will only use activities that a teacher or suitable adult has told or allowed me to use
- I will take care of computers/tablets and other equipment
- I will ask for help from a teacher or suitable adult if I am not sure what to do or if I think I have done something wrong
- I will tell a teacher or suitable adult 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): ---

Appendix C - Use of Cloud Systems (HWB and additional services) Permission Form – not needed (opt out).

Name: Form: Username:

Hwb Additional Services for Learners – Consent Form for Learners (aged 13+)

Overview

Hwb is an online platform which gives all teachers and learners access to a wide range of bilingual digital tools and resources to support teaching and learning. Many of the resources are available to the public at https://hwb.gov.wales. Hwb is funded and managed by the Welsh Government for the benefit of all maintained schools in Wales.

During 2018/2019 the Welsh Government's statutory **National Reading and Numeracy Tests** will begin the transition (over a three-year period) to **personalised assessments**, eventually replacing the current paper-based national tests. All learners must be provided with a secure 'Hwb login' in preparation for these online assessments and our school will securely send specific information (as detailed in the Hwb Privacy Notice) to the Welsh Government to facilitate this.

Hwb Additional Services

As well as enabling pupils to access personalised assessments, the Welsh Government offers, through Hwb, additional educational services to every learner. You will benefit from online access (on any web connected device) to educational resources including Microsoft 365 (including Word, Excel and Outlook e-mail), Google G Suite for Education, Encyclopaedia Britannica, Just2easy, Flipgrid and other relevant educational tools and resources. The Welsh Government fully supports the use of these educational resources and there is no cost to you or to our school to use them.

In order to access these additional services, we NEED YOUR CONSENT. A video about learner consent is available at https://hwb.gov.wales/consent.

Giving consent / withdrawing consent – how will this affect my Hwb account?

You may give consent or withdraw consent for **Hwb Additional Services** at any time.

If you tick box (a) below and sign to give your consent:

- We will enable you to have access to all the Hwb Additional Services. This will involve Welsh Government securely sharing limited information about you with its service providers, including Microsoft and Google for Education, in order to create a secure account to enable you to access the additional services (see the **Hwb Privacy Notice** at https://hwb.gov.wales/privacy for more details).

If you tick box (b) below and sign to indicate that you **do not** give your consent:

- We will still securely share specific information about you with Welsh Government, and some of its service providers, in order to set up a secure log-in for the Hwb platform to facilitate personalised assessments. However, you **will not be able to access Hwb Additional Services**. Please discuss this further with a teacher.

Hwb

For more information about Hwb and how information about you is used, please visit https://hwb.gov.wales, https://hwb.gov.wales/termsandconditions and https://hwb.gov.wales/privacy.

Personalised Assessments

For more information please visit https://hwb.gov.wales/personalised-assessments.

Learner (aged 13+) Consent (Hwb)

Please tick the appropriate box below, complete the details and return to the school office as soon as possible.

□ (a) I consent to accessing **Hwb Additional Services**

□ (b) I **do not** consent to accessing **Hwb Additional Services**

Learner's Full Name: .... Learner's Year Group: ....

Signed: .... Date: ....

Name: Form: Username:

Hwb Additional Services for Learners - Parent/Carer Consent Form

Overview

Hwb is an online platform which gives all teachers and learners access to a wide range of bilingual digital tools and resources to support teaching and learning. Many of the resources are available to the public at https://hwb.gov.wales and parents/carers are encouraged to visit the website. Hwb is funded and managed by the Welsh Government for the benefit of all maintained schools in Wales.

During 2018/2019 the Welsh Government's statutory **National Reading and Numeracy Tests** will begin the transition (over a three-year period) to **personalised assessments**, eventually replacing the current paper-based national tests. All learners must be provided with a secure 'Hwb login' in preparation for these online assessments and our school will securely send specific information (as detailed in the Hwb Privacy Notice) to the Welsh Government to facilitate this.

Hwb Additional Services

As well as facilitating the personalised assessments, the Welsh Government offers, through Hwb, additional educational services to every learner. Your child will benefit from online access (on any web connected device) to educational resources including Microsoft 365 (including Word, Excel and Outlook e-mail), Google G Suite for Education, Encyclopaedia Britannica, Just2easy, Flipgrid and other relevant educational tools and resources. The Welsh Government fully supports the use of these educational resources and there is no cost to you or to our school for your child to use them.

In order to enable your child to access these additional services, we need you to give your consent. A video about learner consent is available at https://hwb.gov.wales/consent.

Giving consent / withdrawing consent – how will this affect my child's Hwb account?

You may give consent or withdraw consent for **Hwb Additional Services** at any time.

If you tick box (a) below and sign to give your consent:

- We will enable your child to have access to all the Hwb Additional Services. This will involve Welsh Government securely sharing limited information about your child with its service providers, including Microsoft and Google for Education, in order to create a secure account to enable them to access the additional services (see the **Hwb Privacy Notice** at https://hwb.gov.wales/privacy for more details).

If you tick box (b) below and sign to indicate that you **do not** give your consent:

- We will still securely share specific information about your child with Welsh Government, and some of its service providers, in order to set up a secure log-in for the Hwb platform to facilitate personalised assessments. However, your child **will not be able to access Hwb Additional Services**. Please contact your child's class teacher to discuss further.

Hwb

For more information about Hwb and how information about your child is used, please visit https://hwb.gov.wales, https://hwb.gov.wales/termsandconditions and https://hwb.gov.wales/privacy.

Personalised Assessments

For more information please visit https://hwb.gov.wales/personalised-assessments.

Parent/Carer Consent (Hwb) Ysgol Bro Gwaun

Please tick the appropriate box below, complete the details and return to the school office as soon as possible.

□ (a) I consent to my child accessing **Hwb Additional Services**

□ (b) I **do not** consent to my child accessing **Hwb Additional Services**

Learner's Name: .... Learner's Year Group: ....

Signed: .... Date: ....

Please print <u>your</u> name: ....

Please indicate your relationship to the learner: ....

Appendix D - Staff (and Volunteer) Acceptable Use Policy Agreement Template

School Policy

New technologies have become integral to the lives of children and young people in today's society, both within schools/academies and in their lives outside school. The internet and other digital information and communications technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. They also bring opportunities for staff to be more creative and productive in their work. All users should have an entitlement to safe access to the internet and digital technologies at all times.

This acceptable use policy is intended to ensure:

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

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

Acceptable Use Policy Agreement

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

For my professional and personal safety:

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

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

- I will not access, copy, remove or otherwise alter any other user's files, without their express permission.
- I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will ensure that when I take and/or publish images of others I will do so with their permission and in accordance with the school's policy on the use of digital/video images. I will not use my personal equipment to record these images, unless I have permission to do so. Where these images are published (e.g. on the school website/VLE) it will not be possible to identify by name, or other personal information, those who are featured.

- I will only use social networking sites in school in accordance with the school's policies.
- I will only communicate with students/pupils and parents/carers using official school systems. Any such communication will be professional in tone and manner.
- I will not engage in any on-line activity that may compromise my professional responsibilities.

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

- When I use my mobile devices in school, I will follow the rules set out in this agreement, in the same way as if I was using *school* equipment. I will also follow any additional rules set by the *school* about such use. I will ensure that any such devices are protected by up to date anti-virus software and are free from viruses.
- I will not open any hyperlinks in emails or any attachments to emails, unless the source is known and trusted, or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes) and will report suspicious content/links to the Network Manager.
- 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, terrorist or extremist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering/security systems in place to prevent access to such materials.
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings, unless this is allowed in school policies.
- I will not disable or cause any damage to school equipment, or the equipment belonging to others.
- I will only transport, hold, disclose or share personal information about myself or others, as outlined in the School/LA Personal Data Policy (or other relevant policy). Where digital personal data is transferred outside the secure local network, it must be encrypted. Paper based documents containing personal data must be held in lockable storage.
- I understand that data protection policy requires that any staff or student/pupil data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by school 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 and where appropriate attribute rights to the work of others.
- Where work is protected by copyright, I will not download or distribute copies (including music and videos).

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

- I understand that this acceptable use policy applies not only to my work and use of school digital technology equipment in school, 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
- 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/directors and/or the Local Authority and in the event of illegal activities the involvement of the police.

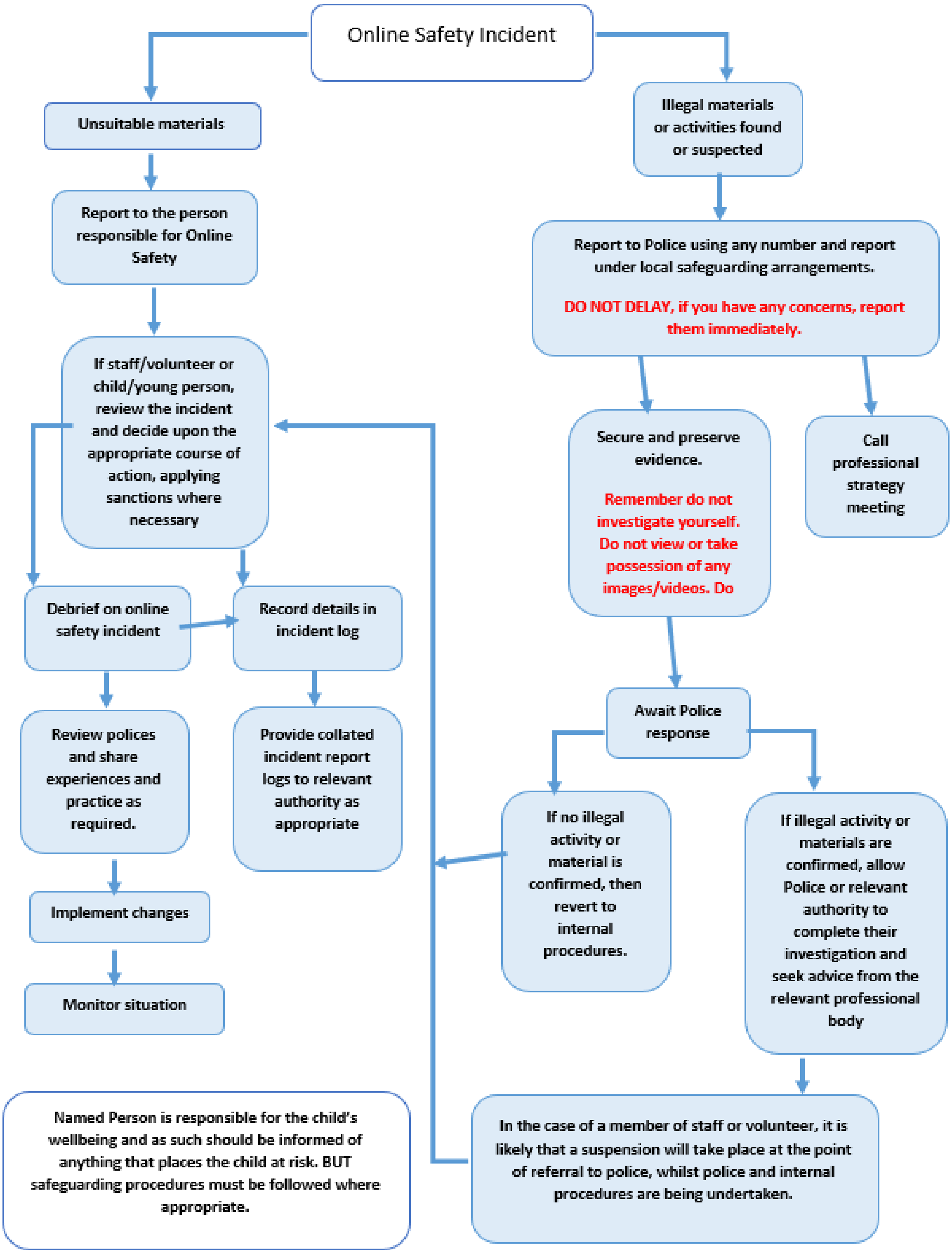
I have read and understand the above and agree to use the school digital technology systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) within these guidelines.

Staff/Volunteer Name: --

Signed: --

Date: --

Appendix E - Responding to incidents of misuse – flow chart



Online Safety Incident

Unsuitable materials

Report to the person responsible for Online Safety

If staff/volunteer or child/young person, review the incident and decide upon the appropriate course of action, applying sanctions where necessary

Debrief on online safety incident

Record details in incident log

Review polices and share experiences and practice as required.

Provide collated incident report logs to relevant authority as appropriate

Implement changes

Monitor situation

Illegal materials or activities found or suspected

Report to Police using any number and report under local safeguarding arrangements.

DO NOT DELAY, if you have any concerns, report them immediately.

Secure and preserve evidence.

Remember do not investigate yourself. Do not view or take possession of any images/videos. Do

Call professional strategy meeting

Await Police response

If no illegal activity or material is confirmed, then revert to internal procedures.

If illegal activity or materials are confirmed, allow Police or relevant authority to complete their investigation and seek advice from the relevant professional body

In the case of a member of staff or volunteer, it is likely that a suspension will take place at the point of referral to police, whilst police and internal procedures are being undertaken.

Named Person is responsible for the child's wellbeing and as such should be informed of anything that places the child at risk. BUT safeguarding procedures must be followed where appropriate.

Appendix F - Record of reviewing devices/internet sites (responding to incidents of misuse)

Group: ....

Date: ....

Reason for investigation: ....

....

....

Details of first reviewing person

Name: ....

Position: ....

Signature: ....

Details of second reviewing person

Name: ....

Position: ....

Signature: ....

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

....

....

Web site(s) address/device	Reason for concern

Conclusion and Action proposed or taken

Review: Look at creating an online form for this.

Appendix G - Training Needs Audit Log – look to make digital form

Group: ....

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

Appendix H - School Policy 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 may include:

- SLT member/s
- Child Protection/Safeguarding officer
- Teaching staff member
- Support staff member
- Online safety coordinator (not ICT coordinator by default)
- Governor
- Parent/Carer
- ICT Technical Support staff (where possible)
- Community users (where appropriate)
- Digital Leaders
- School Council

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

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

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

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

3. Chairperson

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

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

4. Duration of Meetings

Meetings shall be held half-termly 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 Lead (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 [add/delete as relevant]:
- Staff meetings
- Student/pupil forums (for advice and feedback)
- Governors meetings
- Surveys/questionnaires for students/pupils, parents/carers and staff
- Parents evenings
- Website/VLE/Newsletters
- Online safety events
- Online 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
- 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 committee members, by agreement of the majority

The above Terms of Reference for YBG Online Safety Group have been agreed

Signed by (SLT): --

Date: --

Date for review: --

Acknowledgement

This template terms of reference document are based on one provided to schools/academies by Somerset County Council

Appendix I - Legislation

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

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

Computer Misuse Act 1990

This Act makes it an offence to:

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

School/academies may wish to view the National Crime Agency website which includes information about "Cyber crime – preventing young people from getting involved". Each region in England (& Wales) has a Regional Organised Crime Unit (ROCU) Cyber-Prevent team that works with schools to encourage young people to make positive use of their cyber skills. There is a useful summary of the Act on the NCA site.

Data Protection Act 1998

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

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

The Data Protection Act 2018:

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

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

All data subjects have the right to:

- Receive clear information about what you will use their data for.

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

Freedom of Information Act 2000

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

Communications Act 2003

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

Malicious Communications Act 1988

It is an offence to send an indecent, offensive, or threatening letter, electronic communication or another article to another person.

Regulation of Investigatory Powers Act 2000

It is an offence for any person to intentionally and without lawful authority intercept any communication. Monitoring or keeping a record of any form of electronic communications is permitted, in order to:

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

Trade Marks Act 1994

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

Copyright, Designs and Patents Act 1988

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

Telecommunications Act 1984

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

Criminal Justice & Public Order Act 1994

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

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

Racial and Religious Hatred Act 2006

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

Protection from Harassment Act 1997

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

Protection of Children Act 1978

It is an offence to take, permit to be taken, make, possess, show, distribute or advertise indecent images of children in the United Kingdom. A child for these purposes is anyone under the age of 18. Viewing an indecent image of a child on your computer means that you have made a digital image. An image of a child also covers pseudo-photographs (digitally collated or otherwise). A person convicted of such an offence may face up to 10 years in prison

Sexual Offences Act 2003

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

Public Order Act 1986

This Act makes it a criminal offence to stir up racial hatred by displaying, publishing or distributing written material which is threatening. Like the Racial and Religious Hatred Act 2006 it also makes the possession of inflammatory material with a view of releasing it a criminal offence. Children, Families and Education Directorate page 38 April 2007.

Obscene Publications Act 1959 and 1964

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

Human Rights Act 1998

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

- The right to a fair trial

- The right to respect for private and family life, home and correspondence
- Freedom of thought, conscience and religion
- Freedom of expression
- Freedom of assembly
- Prohibition of discrimination
- The right to education

These rights are not absolute. The school is obliged to respect these rights and freedoms, balancing them against those rights, duties and obligations, which arise from other relevant legislation.

The Protection of Freedoms Act 2012

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

The School Information Regulations 2012

Requires schools to publish certain information on its website:

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

Serious Crime Act 2015

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

Criminal Justice and Courts Act 2015

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

For further guidance or support please contact the Revenge Porn Helpline

Appendix J - Links to other organisations or documents

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

UK Safer Internet Centre

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

South West Grid for Learning - https://swgfl.org.uk/products-services/onlinOnline Safety/

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

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

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

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

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

CEOP

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

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

Others

LGfL – Online Safety Resources

Kent – Online Safety Resources page

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

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

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

Tools for Schools

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

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

360Data – online data protection self-review tool: www.360data.org.uk

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

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

Bullying/Online-bullying/Sexting/Sexual Harassment

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

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

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

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

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

Childnet – Cyberbullying guidance and practical PSHE toolkit:

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

Childnet – Project deSHAME – Online Sexual Harrassment

UKSIC – Sexting Resources

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

Ditch the Label – Online Bullying Charity

Diana Award – Anti-Bullying Campaign

Social Networking

Digizen – Social Networking

UKSIC - Safety Features on Social Networks

Children's Commissioner, TES and Schillings – Young peoples' rights on social media

Curriculum

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

UKCCIS – Education for a connected world framework

Teach Today – www.teachtoday.eu/

Insafe - Education Resources

Data Protection

360data - free questionnaire and data protection self review tool

ICO Guides for Education (wide range of sector specific guides)

DfE advice on Cloud software services and the Data Protection Act

IRMS - Records Management Toolkit for Schools

NHS - Caldicott Principles (information that must be released)

ICO Guidance on taking photos in schools

Dotkumo - Best practice guide to using photos

Professional Standards/Staff Training

DfE – Keeping Children Safe in Education

DfE - Safer Working Practice for Adults who Work with Children and Young People

Childnet – School Pack for Online Safety Awareness

UK Safer Internet Centre Professionals Online Safety Helpline

Infrastructure/Technical Support

UKSIC – Appropriate Filtering and Monitoring

SWGfL Safety & Security Resources

Somerset - Questions for Technical Support

NCA – Guide to the Computer Misuse Act

NEN – Advice and Guidance Notes

Working with parents and carers

Online Safety BOOST Presentations - parent's presentation

Vodafone Digital Parents Magazine

Childnet Webpages for Parents & Carers

Get Safe Online - resources for parents

Teach Today - resources for parents workshops/education

Internet Matters

Prevent

Prevent Duty Guidance
Prevent for schools – teaching resources
NCA – Cyber Prevent
Childnet – Trust Me

Research

Ofcom –Media Literacy Research

Further links can be found at the end of the UKCIS Education for a Connected World Framework

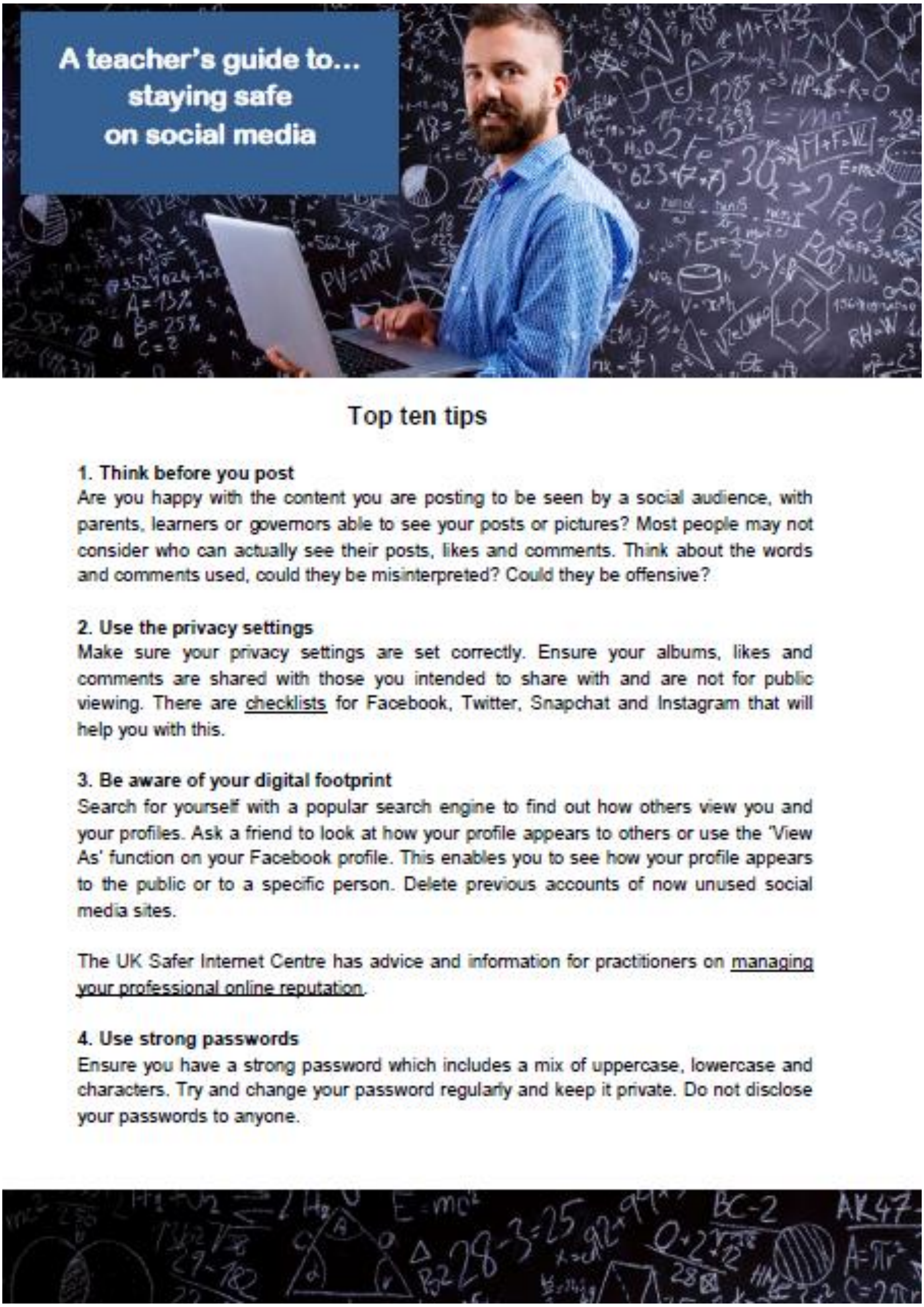
Appendix K - Glossary of Terms

AUP/AUA	Acceptable Use Policy/Agreement – see templates earlier in this document
CEOP	Child Exploitation and Online Protection Centre (part of National Crime Agency, 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
ICO	Information Commissioners Office
ICT	Information and Communications Technology
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
MAT	Multi Academy Trust
MIS	Management Information System
NEN	National Education Network – works with the Regional Broadband Consortia (e.g. SWGfL) to provide the safe broadband provision to schools across Britain.
Ofcom	Office of Communications (Independent communications sector regulator)
SWGfL	South West Grid for Learning Trust – the Regional Broadband Consortium of SW Local Authorities – is the provider of broadband and other services for schools and other organisations in the SW
TUK	Think U Know – educational online safety programmes for schools, young people and parents.
UKSIC	UK Safer Internet Centre – EU funded centre. Main partners are SWGfL, Childnet and Internet Watch Foundation.
UKCIS	UK Council for Online Safety
VLE	Virtual Learning Environment (a software system designed to support teaching and learning in an educational setting,
WAP	Wireless Application Protocol

A more comprehensive glossary can be found at the end of the UKCIS Education for a Connected World Framework

Every reasonable effort has been made to ensure that the information included in this template is accurate, as at the date of publication in January 2020. 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.

Appendix L – A teachers guide to staying safe on social media



A teacher's guide to... staying safe on social media

Top ten tips

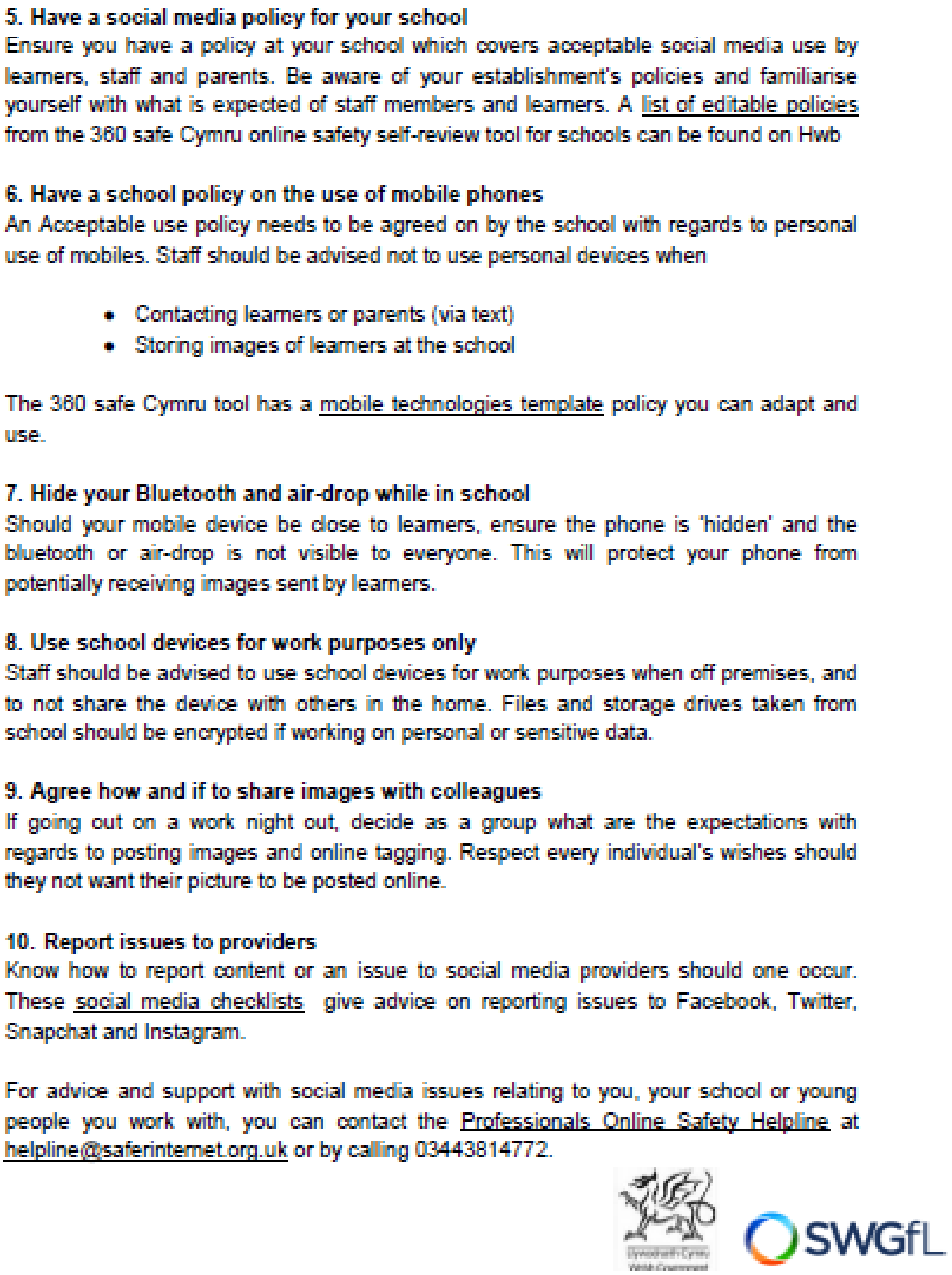
1. Think before you post
Are you happy with the content you are posting to be seen by a social audience, with parents, learners or governors able to see your posts or pictures? Most people may not consider who can actually see their posts, likes and comments. Think about the words and comments used, could they be misinterpreted? Could they be offensive?

2. Use the privacy settings
Make sure your privacy settings are set correctly. Ensure your albums, likes and comments are shared with those you intended to share with and are not for public viewing. There are checklists for Facebook, Twitter, Snapchat and Instagram that will help you with this.

3. Be aware of your digital footprint
Search for yourself with a popular search engine to find out how others view you and your profiles. Ask a friend to look at how your profile appears to others or use the 'View As' function on your Facebook profile. This enables you to see how your profile appears to the public or to a specific person. Delete previous accounts of now unused social media sites.

The UK Safer Internet Centre has advice and information for practitioners on managing your professional online reputation.

4. Use strong passwords
Ensure you have a strong password which includes a mix of uppercase, lowercase and characters. Try and change your password regularly and keep it private. Do not disclose your passwords to anyone.



5. Have a social media policy for your school

Ensure you have a policy at your school which covers acceptable social media use by learners, staff and parents. Be aware of your establishment's policies and familiarise yourself with what is expected of staff members and learners. A list of editable policies from the 360 safe Cymru online safety self-review tool for schools can be found on Hwb

6. Have a school policy on the use of mobile phones

An Acceptable use policy needs to be agreed on by the school with regards to personal use of mobiles. Staff should be advised not to use personal devices when

- Contacting learners or parents (via text)
- Storing images of learners at the school

The 360 safe Cymru tool has a mobile technologies template policy you can adapt and use.

7. Hide your Bluetooth and air-drop while in school

Should your mobile device be close to learners, ensure the phone is 'hidden' and the bluetooth or air-drop is not visible to everyone. This will protect your phone from potentially receiving images sent by learners.

8. Use school devices for work purposes only

Staff should be advised to use school devices for work purposes when off premises, and to not share the device with others in the home. Files and storage drives taken from school should be encrypted if working on personal or sensitive data.

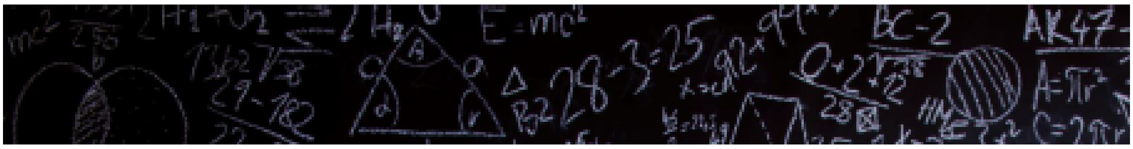
9. Agree how and if to share images with colleagues

If going out on a work night out, decide as a group what are the expectations with regards to posting images and online tagging. Respect every individual's wishes should they not want their picture to be posted online.

10. Report issues to providers

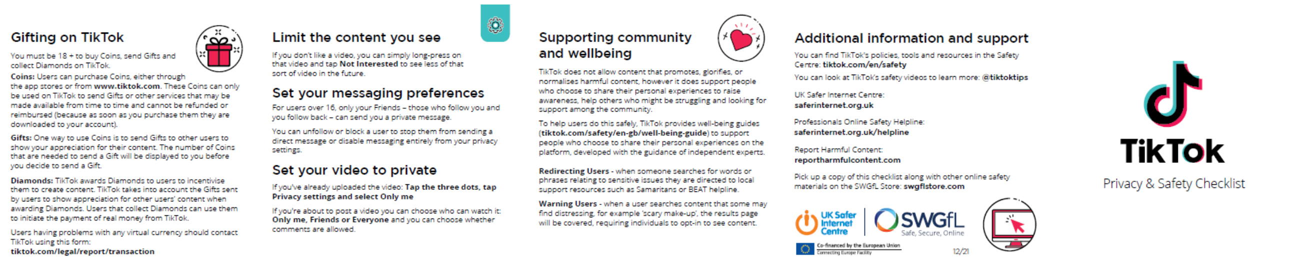
Know how to report content or an issue to social media providers should one occur. These social media checklists give advice on reporting issues to Facebook, Twitter, Snapchat and Instagram.

For advice and support with social media issues relating to you, your school or young people you work with, you can contact the Professionals Online Safety Helpline at helpline@saferinternet.org.uk or by calling 03443814772.



https://hwb.gov.wales/zones/keeping-safe-online/resources/a-teacher-s-guide-to-staying-safe-on-social-media#:~:text=Use%20the%20privacy%20settings,will%20help%20you%20with%20this

Appendix M – Social Media Checklists



Gifting on TikTok

You must be 18 + to buy Coins, send Gifts and collect Diamonds on TikTok.

Coins: Users can purchase Coins, either through the app stores or from **www.tiktok.com**. These Coins can only be used on TikTok to send Gifts or other services that may be made available from time to time and cannot be refunded or reimbursed (because as soon as you purchase them they are downloaded to your account).

Gifts: One way to use Coins is to send Gifts to other users to show your appreciation for their content. The number of Coins that are needed to send a Gift will be displayed to you before you decide to send a Gift.

Diamonds: TikTok awards Diamonds to users to incentivise them to create content. TikTok takes into account the Gifts sent by users to show appreciation for other users' content when awarding Diamonds. Users that collect Diamonds can use them to initiate the payment of real money from TikTok.

Users having problems with any virtual currency should contact TikTok using this form: **tiktok.com/legal/report/transaction**

Limit the content you see

If you don't like a video, you can simply long-press on that video and tap **Not Interested** to see less of that sort of video in the future.

Set your messaging preferences

For users over 16, only your Friends – those who follow you and you follow back – can send you a private message.

You can unfollow or block a user to stop them from sending a direct message or disable messaging entirely from your privacy settings.

Set your video to private

If you've already uploaded the video: **Tap the three dots, tap Privacy settings and select Only me**

If you're about to post a video you can choose who can watch it: **Only me, Friends or Everyone** and you can choose whether comments are allowed.

Supporting community and wellbeing

TikTok does not allow content that promotes, glorifies, or normalises harmful content, however it does support people who choose to share their personal experiences to raise awareness, help others who might be struggling and looking for support among the community.

To help users do this safely, TikTok provides well-being guides (**tiktok.com/safety/en-gb/well-being-guide**) to support people who choose to share their personal experiences on the platform, developed with the guidance of independent experts.

Redirecting Users - when someone searches for words or phrases relating to sensitive issues they are directed to local support resources such as Samaritans or BEAT helpline.

Warning Users - when a user searches content that some may find distressing, for example 'scary make-up', the results page will be covered, requiring individuals to opt-in to see content.

Additional information and support

You can find TikTok's policies, tools and resources in the Safety Centre: **tiktok.com/en/safety**

You can look at TikTok's safety videos to learn more: **@tiktoktips**

UK Safer Internet Centre:
saferinternet.org.uk

Professionals Online Safety Helpline:
saferinternet.org.uk/helpline

Report Harmful Content:
reportharmfulcontent.com

Pick up a copy of this checklist along with other online safety materials on the SWGfL Store: **swgflstore.com**

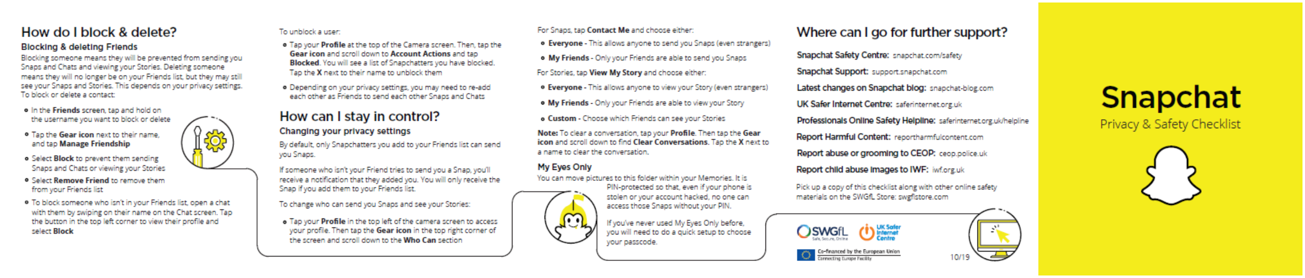
UK Safer Internet Centre | SWGfL Safe, Secure, Online

Co-financed by the European Union
Connecting Europe Facility

12/21

TikTok

Privacy & Safety Checklist



How do I block & delete?

Blocking & deleting Friends

Blocking someone means they will be prevented from sending you Snaps and Chats and viewing your Stories. Deleting someone means they will no longer be on your Friends list, but they may still see your Snaps and Stories. This depends on your privacy settings. To block or delete a contact:

- In the **Friends** screen, tap and hold on the username you want to block or delete
- Tap the **Gear icon** next to their name, and tap **Manage Friendship**
- Select **Block** to prevent them sending Snaps and Chats or viewing your Stories
- Select **Remove Friend** to remove them from your Friends list
- To block someone who isn't in your Friends list, open a chat with them by swiping on their name on the Chat screen. Tap the button in the top left corner to view their profile and select **Block**

To unblock a user:

- Tap your **Profile** at the top of the Camera screen. Then, tap the **Gear icon** and scroll down to **Account Actions** and tap **Blocked**. You will see a list of Snapchatters you have blocked. Tap the **X** next to their name to unblock them
- Depending on your privacy settings, you may need to re-add each other as Friends to send each other Snaps and Chats

How can I stay in control?

Changing your privacy settings

By default, only Snapchatters you add to your Friends list can send you Snaps.

If someone who isn't your Friend tries to send you a Snap, you'll receive a notification that they added you. You will only receive the Snap if you add them to your Friends list.

To change who can send you Snaps and see your Stories:

- Tap your **Profile** in the top left of the camera screen to access your profile. Then tap the **Gear icon** in the top right corner of the screen and scroll down to the **Who Can** section

For Snaps, tap **Contact Me** and choose either:

- **Everyone** - This allows anyone to send you Snaps (even strangers)
- **My Friends** - Only your Friends are able to send you Snaps

For Stories, tap **View My Story** and choose either:

- **Everyone** - This allows anyone to view your Story (even strangers)
- **My Friends** - Only your Friends are able to view your Story
- **Custom** - Choose which Friends can see your Stories

Note: To clear a conversation, tap your **Profile**. Then tap the **Gear icon** and scroll down to find **Clear Conversations.** Tap the **X** next to a name to clear the conversation.

My Eyes Only

You can move pictures to this folder within your Memories. It is PIN-protected so that, even if your phone is stolen or your account hacked, no one can access those Snaps without your PIN.

If you've never used My Eyes Only before, you will need to do a quick setup to choose your passcode.

Where can I go for further support?

Snapchat Safety Centre: snapchat.com/safety

Snapchat Support: support.snapchat.com

Latest changes on Snapchat blog: snapchat-blog.com

UK Safer Internet Centre: saferinternet.org.uk

Professionals Online Safety Helpline: saferinternet.org.uk/helpline

Report Harmful Content: reportharmfulcontent.com

Report abuse or grooming to CEOP: ceop.police.uk

Report child abuse images to IWF: iwf.org.uk

Pick up a copy of this checklist along with other online safety materials on the SWGfL Store: swgflstore.com

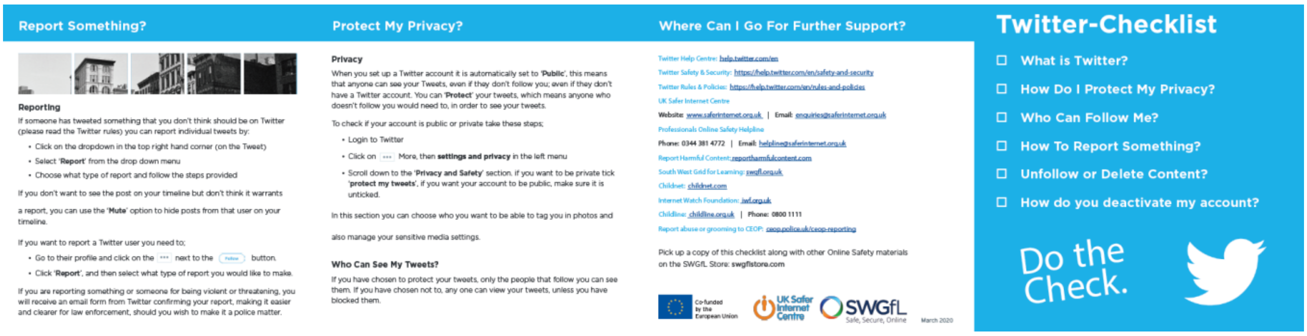
SWGfL UK Safer Internet Centre

Co-financed by the European Union
Connecting Europe Facility

10/19

Snapchat

Privacy & Safety Checklist



Report Something?

Reporting

If someone has tweeted something that you don't think should be on Twitter (please read the Twitter rules) you can report individual tweets by:

- Click on the dropdown in the top right hand corner (on the Tweet)
- Select '**Report**' from the drop down menu
- Choose what type of report and follow the steps provided

If you don't want to see the post on your timeline but don't think it warrants

a report, you can use the '**Mute**' option to hide posts from that user on your timeline.

If you want to report a Twitter user you need to;

- Go to their profile and click on the ••• next to the Follow button.
- Click '**Report**', and then select what type of report you would like to make.

If you are reporting something or someone for being violent or threatening, you will receive an email form from Twitter confirming your report, making it easier and clearer for law enforcement, should you wish to make it a police matter.

Protect My Privacy?

Privacy

When you set up a Twitter account it is automatically set to '**Public**', this means that anyone can see your Tweets, even if they don't follow you; even if they don't have a Twitter account. You can '**Protect**' your tweets, which means anyone who doesn't follow you would need to, in order to see your tweets.

To check if your account is public or private take these steps;

- Login to Twitter
- Click on ••• More, then **settings and privacy** in the left menu
- Scroll down to the '**Privacy and Safety**' section. If you want to be private tick '**protect my tweets**', if you want your account to be public, make sure it is unticked.

In this section you can choose who you want to be able to tag you in photos and

also manage your sensitive media settings.

Who Can See My Tweets?

If you have chosen to protect your tweets, only the people that follow you can see them. If you have chosen not to, any one can view your tweets, unless you have blocked them.

Where Can I Go For Further Support?

Twitter Help Centre: help.twitter.com/en

Twitter Safety & Security: https://help.twitter.com/en/safety-and-security

Twitter Rules & Policies: https://help.twitter.com/en/rules-and-policies

UK Safer Internet Centre

Website: www.saferinternet.org.uk | Email: enquiries@saferinternet.org.uk

Professionals Online Safety Helpline

Phone: 0344 381 4772 | Email: helpline@saferinternet.org.uk

Report Harmful Content: reportharmfulcontent.com

South West Grid for Learning: swgfl.org.uk

Childnet: childnet.com

Internet Watch Foundation: iwf.org.uk

Childline: childline.org.uk | Phone: 0800 1111

Report abuse or grooming to CEOP: ceop.police.uk/ceop-reporting

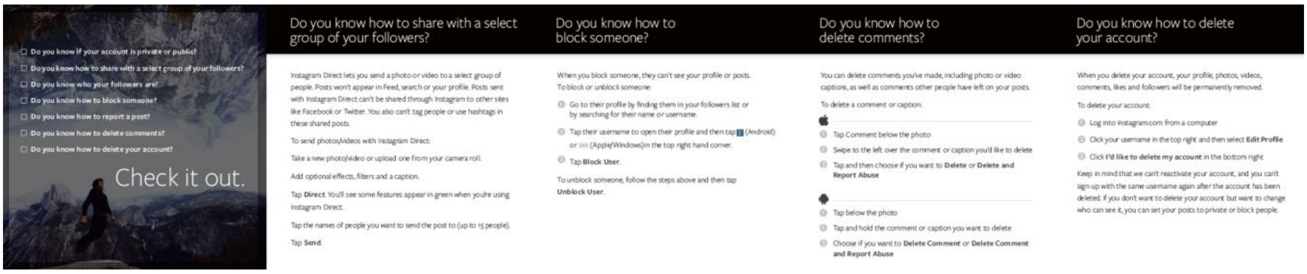
Pick up a copy of this checklist along with other Online Safety materials on the SWGfL Store: swgflstore.com

Co-funded by the European Union | UK Safer Internet Centre | SWGfL Safe, Secure, Online | March 2020

Twitter-Checklist

- □ What is Twitter?
- □ How Do I Protect My Privacy?
- □ Who Can Follow Me?
- □ How To Report Something?
- □ Unfollow or Delete Content?
- □ How do you deactivate my account?

Do the Check.



- □ Do you know if your account is private or public?
- □ Do you know how to share with a select group of your followers?
- □ Do you know who your followers are?
- □ Do you know how to block someone?
- □ Do you know how to report a post?
- □ Do you know how to delete comments?
- □ Do you know how to delete your account?

Check it out.

Do you know how to share with a select group of your followers?

Instagram Direct lets you send a photo or video to a select group of people. Posts won't appear in Feed, search or your profile. Posts sent with Instagram Direct can't be shared through Instagram to other sites like Facebook or Twitter. You also can't tag people or use hashtags in these shared posts.

To send photos/videos with Instagram Direct:

Take a new photo/video or upload one from your camera roll.

Add optional effects, filters and a caption.

Tap **Direct**. You'll see some features appear in green when you're using Instagram Direct.

Tap the names of people you want to send the post to (up to 15 people).

Tap **Send**.

Do you know how to block someone?

When you block someone, they can't see your profile or posts.
To block or unblock someone:

- Go to their profile by finding them in your followers list or by searching for their name or username.
- Tap their username to open their profile and then tap ⋮ (Android) or ••• (Apple/Windows)in the top right hand corner.
- Tap **Block User**.

To unblock someone, follow the steps above and then tap **Unblock User**.

Do you know how to delete comments?

You can delete comments you've made, including photo or video captions, as well as comments other people have left on your posts.

To delete a comment or caption:

- Tap Comment below the photo
- Swipe to the left over the comment or caption you'd like to delete
- Tap and then choose if you want to **Delete** or **Delete and Report Abuse**

- Tap below the photo
- Tap and hold the comment or caption you want to delete
- Choose if you want to **Delete Comment** or **Delete Comment and Report Abuse**

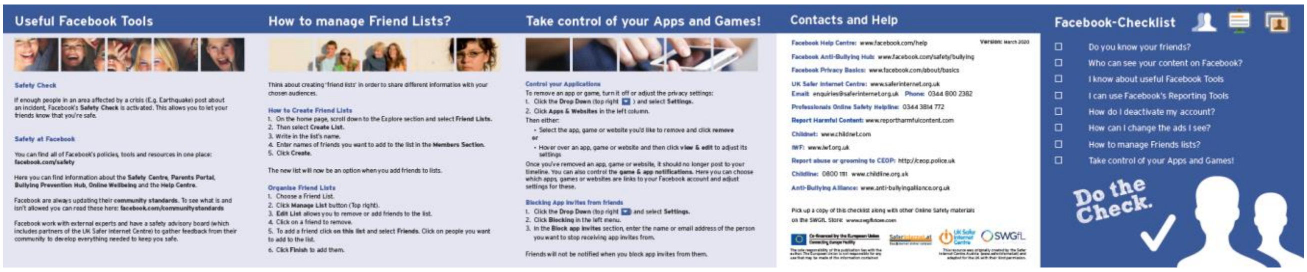
Do you know how to delete your account?

When you delete your account, your profile, photos, videos, comments, likes and followers will be permanently removed.

To delete your account:

- Log into instagram.com from a computer
- Click your username in the top right and then select **Edit Profile**
- Click **I'd like to delete my account** in the bottom right

Keep in mind that we can't reactivate your account, and you can't sign up with the same username again after the account has been deleted. If you don't want to delete your account but want to change who can see it, you can set your posts to private or block people.



Useful Facebook Tools

Safety Check

If enough people in an area affected by a crisis (E.g. Earthquake) post about an incident, Facebook's **Safety Check** is activated. This allows you to let your friends know that you're safe.

Safety at Facebook

You can find all of Facebook's policies, tools and resources in one place: **facebook.com/safety**

Here you can find information about the **Safety Centre, Parents Portal, Bullying Prevention Hub, Online Wellbeing** and the **Help Centre.**

Facebook are always updating their **community standards**. To see what is and isn't allowed you can read these here: **facebook.com/communitystandards**

Facebook work with external experts and have a safety advisory board (which includes partners of the UK Safer Internet Centre) to gather feedback from their community to develop everything needed to keep you safe.

How to manage Friend Lists?

Think about creating 'friend lists' in order to share different information with your chosen audiences.

How to Create Friend Lists

1. On the home page, scroll down to the Explore section and select **Friend Lists.**
2. Then select **Create List.**
3. Write in the list's name.
4. Enter names of friends you want to add to the list in the **Members Section.**
5. Click **Create.**

The new list will now be an option when you add friends to lists.

Organise Friend Lists

1. Choose a Friend List.
2. Click **Manage List** button (Top right).
3. **Edit List** allows you to remove or add friends to the list.
4. Click on a friend to remove.
5. To add a friend click **on this list** and select **Friends.** Click on people you want to add to the list.
6. Click **Finish** to add them.

Take control of your Apps and Games!

Control your Applications

To remove an app or game, turn it off or adjust the privacy settings:

1. Click the **Drop Down** (top right ▾) and select **Settings.**
2. Click **Apps & Websites** in the left column.

Then either:

- Select the app, game or website you'd like to remove and click **remove**

or

- Hover over an app, game or website and then click **view & edit** to adjust its settings

Once you've removed an app, game or website, it should no longer post to your timeline. You can also control the **game & app notifications.** Here you can choose which apps, games or websites are links to your Facebook account and adjust settings for these.

Blocking App Invites from friends

1. Click the **Drop Down** (top right ▾) and select **Settings.**
2. Click **Blocking** in the left menu.
3. In the **Block app invites** section, enter the name or email address of the person you want to stop receiving app invites from.

Friends will not be notified when you block app invites from them.

Contacts and Help

Version: March 2020

Facebook Help Centre: www.facebook.com/help

Facebook Anti-Bullying Hub: www.facebook.com/safety/bullying

Facebook Privacy Basics: www.facebook.com/about/basics

UK Safer Internet Centre: www.saferinternet.org.uk

Email: enquiries@saferinternet.org.uk **Phone:** 0344 800 2382

Professionals Online Safety Helpline: 0344 3814 772

Report Harmful Content: www.reportharmfulcontent.com

Childnet: www.childnet.com

IWF: www.iwf.org.uk

Report abuse or grooming to CEOP: http://ceop.police.uk

Childline: 0800 1111 www.childline.org.uk

Anti-Bullying Alliance: www.anti-bullyingalliance.org.uk

Pick up a copy of this checklist along with other Online Safety materials on the SWGfL Store: www.swgflstore.com

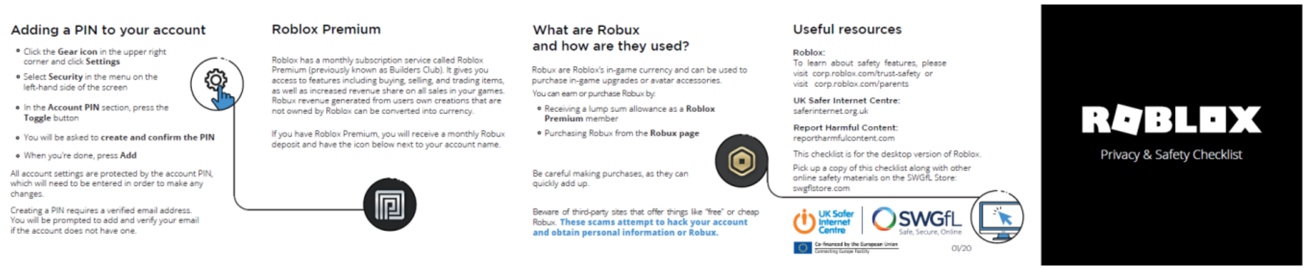
Co-financed by the European Union
Connecting Europe Facility

[illegible]

Facebook-Checklist

- □ Do you know your friends?
- □ Who can see your content on Facebook?
- □ I know about useful Facebook Tools
- □ I can use Facebook's Reporting Tools
- □ How do I deactivate my account?
- □ How can I change the ads I see?
- □ How to manage Friends lists?
- □ Take control of your Apps and Games!

Do the Check. ✓



Adding a PIN to your account

- Click the **Gear icon** in the upper right corner and click **Settings**
- Select **Security** in the menu on the left-hand side of the screen
- In the **Account PIN** section, press the **Toggle** button
- You will be asked to **create and confirm the PIN**
- When you're done, press **Add**

All account settings are protected by the account PIN, which will need to be entered in order to make any changes.

Creating a PIN requires a verified email address. You will be prompted to add and verify your email if the account does not have one.

Roblox Premium

Roblox has a monthly subscription service called Roblox Premium (previously known as Builders Club). It gives you access to features including buying, selling, and trading items, as well as increased revenue share on all sales in your games. Robux revenue generated from users own creations that are not owned by Roblox can be converted into currency.

If you have Roblox Premium, you will receive a monthly Robux deposit and have the icon below next to your account name.

What are Robux and how are they used?

Robux are Roblox's in-game currency and can be used to purchase in-game upgrades or avatar accessories.

You can earn or purchase Robux by:

- Receiving a lump sum allowance as a **Roblox Premium** member
- Purchasing Robux from the **Robux page**

Be careful making purchases, as they can quickly add up.

Beware of third-party sites that offer things like "free" or cheap Robux. **These scams attempt to hack your account and obtain personal information or Robux.**

Useful resources

Roblox:
To learn about safety features, please visit corp.roblox.com/trust-safety or visit corp.roblox.com/parents

UK Safer Internet Centre:
saferinternet.org.uk

Report Harmful Content:
reportharmfulcontent.com

This checklist is for the desktop version of Roblox.

Pick up a copy of this checklist along with other online safety materials on the SWGfL Store: swgflstore.com

UK Safer Internet Centre | SWGfL Safe, Secure, Online

Co-financed by the European Union
Connecting Europe Facility

01/20

ROBLOX

Privacy & Safety Checklist

Appendix N – Incident Log Report

Incident Log 2022-23

Date	User	Device/location	Concern/Incident	Reviewers	Action taken