Ty Gwyn Education Centre

Date of policy:	January 2020
Adopted:	Management Committee meeting:
To be reviewed:	September 2020
Member of staff responsible:	Head/Safeguarding Officer

Contents

Page 3 Roles and responsibilities

Page 5 Policy statements

Page 8 Mobile Technologies

Page 11 Communication Technologies

Page 12 Social Media (also see Social Media Policy)

Page 13 User actions

Roles and responsibilities

The following section outlines the online safety roles and responsibilities of stakeholders within the Ty Gwyn school community.

Management Committee

Members are responsible for the approval of the online safety policy and for reviewing the effectiveness of the policy. This will be carried out using information provided by the Head to the Premises, Health and Safety sub-committee, who will receive regular information about online safety incidents and monitoring reports. A member of the Management Committee is nominated as Safeguarding member and this includes responsibility for on line/e-safety. This includes:

- regular meetings with the Safeguarding Officer (SO) and/or Deputy Safeguarding Officer (DSO)
- regular monitoring of online safety incident forms
- reporting to relevant governors/sub-committee/meeting.

Headteacher and senior leaders

- The headteacher who is also the SO, 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 can be delegated to the DSO in the absence of the SO
- The headteacher and (at least) another member of the senior leadership team should be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff **– this is the DSO.**
- The headteacher/senior leaders are responsible for ensuring that staff receive suitable training to enable them to carry out their online safety roles within classrooms 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 where there are concerns. This is to provide a safety net and also support to those colleagues who may need it.
- The headteacher/senior leaders will receive and consider promptly reports of any incidents of concern from staff, taking HR advice if required.

Online safety coordinator

At Ty Gwyn, the Head holds the role of Safeguarding Officer and the role of on-line safety coordinator. The Assistant Head is the Deputy Safeguarding Officer and deputises for the SO/on line safety coordinator in her absence.

The online safety coordinator:

- leads and promotes on line safety across the school daily
- 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
- liaises with school technical staff
- receives reports of online safety incidents[1] and creates a log of incidents to inform future online safety developments
- meets regularly with the Management Committee Safeguarding member to discuss current issues, review incident logs
- attends relevant meeting/sub-committee of the Management Committee
- reports regularly to headteacher/senior leadership team

Network manager/technical staff

The network manager/technical staff (RCT CBC staff) is responsible for ensuring that:

- the school technical infrastructure is secure and is not open to misuse or malicious attack
- 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
- users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed
- 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
- the use of the network/internet/learning platform/Hwb/remote access/e-mail is regularly monitored in order that any misuse/attempted misuse can be reported to the headteacher/SO/online safety coordinator for investigation/action/sanction
- monitoring software/systems are implemented and updated as agreed within the SLA between school and the LA
- the filtering policy, is applied and updated on a regular basis and its implementation is not the sole responsibility of any single person

Teaching and support staff

These individuals are responsible for ensuring that:

- they have an up-to-date awareness of online safety matters and of the current school online safety policy and practices
- they have read, understood and signed the staff acceptable use agreement (AUA)
- they report any suspected misuse or problem to the Head/SO/online safety coordinator for investigation/action
- all digital communications with learners/parents and carers should be on a professional level and only carried out using official school systems
- online safety issues are embedded in all aspects of the curriculum and other activities
- learners understand and follow the online safety and acceptable use agreements
- learners have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- they monitor the use of digital technologies, mobile devices, cameras, etc., in lessons and other school activities (where allowed) and implement current policies with regard to these devices
- in lessons where internet use is pre-planned learners should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.

School Council

The School Council of Ty Gwyn considers online safety at each meeting and also provides a consultative group that has wide representation from the whole school community to discuss issues around on line safety and internet use. They have a responsibility to raise awareness of issues regarding online safety and reporting feedback re the policy including the impact of initiatives. The School Council will also regularly report to senior leaders.

Learners

These individuals:

- are responsible for using the school digital technology systems in accordance with the learner acceptable use agreement (this should include personal devices – where allowed)
- should 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/college's online safety policy covers their actions out of school, if related to their membership of the school.

Parents and carers

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

- digital and video images taken at school events
- access to parents'/carers' sections of the website (under development)
- their children's personal devices in the school (where this is allowed)

Policy statements

Education – learners

While regulation and technical solutions are very important, their use must be balanced by educating learners to take a responsible approach. The education of learners in online safety is therefore an essential part of the school's online safety provision. Learners need the help and support of the school to recognise and avoid online safety risks and build their resilience.

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

- A planned online safety curriculum across a range of subjects, (e.g. ICT/PSE/DCF) and topic areas which is regularly reviewed
- Key online safety messages should be reinforced as part of a planned programme of assemblies and tutorial/pastoral activities
- Learners should be taught in all lessons to be critically aware of the materials/content they access online and be guided to validate the accuracy of information
- Learners should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Learners should be supported in building resilience to radicalisation by providing a safe environment for debating controversial issues and helping them to understand how they can influence and participate in decision-making.
- Learners should be helped to understand the need for the learner acceptable use agreement and encouraged to adopt safe and responsible use both within and outside school
- Staff should act as good role models in their use of digital technologies the internet and mobile devices
- In lessons where internet use is pre-planned, it is best practice that learners should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches
- Where learners are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit
- It is accepted that from time to time, for good educational reasons, students may need to research topics, (e.g. racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the technical staff (or other nominated person) can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need

Education – parents and carers

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

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

- *curriculum activities*
- *letters, newsletters*
- *progress days (termly)*
- *high profile events/campaigns, e.g. Safer Internet Day*
- *reference to the relevant web sites/publications, e.g.* hwb.wales.gov.uk/ www.saferinternet.org.uk/ www.childnet.com/parents-and-carers (see Appendix for further links/resources)

Education – the wider community

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

- providing family learning courses in use of new digital technologies, digital literacy and online safety
- online safety messages targeted towards grandparents and other relatives as well as parents.
- the school/college learning platform, Hwb, website will provide online safety information for the wider community
- supporting community groups, e.g. early years settings, childminders, youth/sports/voluntary groups to enhance their online safety provision (possibly supporting the group in the use of Online Compass, an online safety self review tool - www.onlinecompass.org.uk).

Education and training – staff/volunteers

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

- **a planned programme of formal online safety training will be made available to staff. This will be regularly updated and reinforced. An audit of the online safety training needs of all staff will be carried out regularly.** *It is expected that some staff will identify online safety as a training need within the performance management process*
- **all new staff should receive online safety training as part of their induction programme, ensuring that they fully understand the school online safety policy and acceptable use agreements.**
- the online safety coordinator will receive regular updates through attendance at external training events, (e.g. from Consortium/SWGfL/LA/other relevant organisations) and by reviewing guidance documents released by relevant organisations
- this online safety policy and its updates will be presented to and discussed by staff in staff/team meetings/INSET days
- the online safety coordinator/officer will provide advice/guidance/training to individuals as required.

Training – Management Committee Members

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

- attendance at training provided by the local authority/National Governors Association/or other relevant organisation, (e.g. SWGfL)
- participation in school training/information sessions for staff or parents (this may include attendance at assemblies/lessons).

Technical – infrastructure/equipment, filtering and monitoring

If the school has a managed ICT service provided by an outside contractor, it is the responsibility of the school/college to ensure that the managed service provider carries out all the online safety measures that would otherwise be the responsibility of the school, as suggested below. It is also important that the managed service provider is fully aware of the school online safety policy/acceptable use agreements.

The school 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. There will be regular reviews and audits of the safety and security of school/college technical systems:

- Servers, wireless systems and cabling must be securely located and physical access restricted
- Good practice in preventing loss of data from ransomware attacks requires a rigorous and verified back-up routine, including the keeping of copies off-site
- **All school networks and system will be protected by secure passwords**
- **The master account passwords for the school systems should be kept in a secure place, e.g. school safe. Two factor authentication is in place.**
- **All users have clearly defined access rights to school technical systems and devices. Details of the access rights available to groups of users will be recorded by the Network Manager (or other person) and will be reviewed, at least annually by the SO.**
- **All users (adults and learners) have responsibility for the security of their username and password, must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security.**
- **Passwords must not be shared with anyone**
- **Each child has a username and password, known to only themselves**
- **Passwords should be long. Good practice highlights that passwords over 12 characters in length are more difficult to crack. Passwords generated by using a combination of unconnected words that are over 16 characters long are extremely difficult to crack. Password length trumps any other special requirements such as uppercase/lowercase letters, number and special characters. Passwords should be easy to remember, but difficult to guess or crack.**
- The Head is responsible for ensuring that software licence logs are accurate and up-to-date and that regular checks are made to reconcile the number of licences purchased against the number of software installations (inadequate licencing could cause the school/college to breach the Copyright Act which could result in fines or unexpected licensing costs).
- Internet access is filtered for all users. Illegal content (child sexual abuse images) is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list. Content lists are regularly updated and internet use is logged and regularly monitored.
- The school has provided enhanced/differentiated user-level filtering (allowing different filtering levels for different ages/stages and different groups of users: staff/learners, etc.).
- Internet filtering should ensure that children are safe from terrorist and extremist material when accessing the internet.
- Where possible, school technical staff regularly monitor and record the activity of users on the school technical systems and users are made aware of this in the acceptable use agreement.
- An appropriate system is in place for users to report any actual/potential technical incident/security breach to the relevant person, as agreed).
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, mobile devices, etc., from accidental or malicious attempts which might threaten the security of the school/college systems and data. These are tested regularly. The school infrastructure and individual workstations are protected by up to date virus software.
- An agreed policy is in place for the provision of temporary access of ‘guests’, (e.g. trainee teachers, supply teachers, visitors) onto the school systems.
- An agreed policy is in place that forbids staff from downloading executable files and installing programmes on school devices.

- Removable devices eg. Memory sticks cannot be added to the network, unless approved as secure by ICT services
- Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured.

Mobile technologies

Mobile technology devices may be school owned/provided or personally owned and might include smartphone, tablet, notebook/laptop or other technology that usually has the capability of utilising the school's wireless network. Such devices can only be added to the school's network by ICT services and this would be limited to staff devices only, with permission.

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

Please see the Acceptable User Agreements for further details regarding this.

	School/college devices				
	School owned for individual use	School/college owned for multiple users	Authorised device[2]	Student owned	Staff owned
Allowed in school/college	Yes	Yes	Yes	Yes	Yes
Full network access	Some users with permission	No	Yes	No	With permission
Internet only	Yes	Yes	Yes	No	With permission
Network access	Yes	Yes	Yes	No	Yes

Personal devices

- Staff , visitors and pupils are permitted to bring personal mobile devices to school
- Staff, visitors and pupils are expected to use these as described in the AUAs
- Staff, visitors and pupils are responsible for the safety and location of their items, school cannot accept any liability for loss or damage
- The above table shows which users can access the school network, it is limited to staff with permission only
- The AUA sets out an agreement where users will be thoughtful re use of network capacity, taking of photographs and their use/storage and consider data protection issues
- Visitors will be informed about school policy
- Education about the safe and responsible use of mobile devices is included in the school online safety education programmes.

Use of digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and learners instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents and carers and learners need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for 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

2

existing employees. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm.

- **When using digital images, staff should inform and educate learners about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet, e.g. on social networking sites**
- 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 *learners* in the digital/video images.
- Staff and volunteers are allowed to take digital/video images to support educational aims (where permission is in place), but must follow school/college policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school/college equipment;, the personal equipment of staff should not be used for such purposes.
- Care should be taken when taking digital/video images that learners are appropriately dressed and are not participating in activities that might bring the individuals or the school/college into disrepute.
- Learners must not take, use, share, publish or distribute images of others without their permission
- Photographs published on the website (where permission is in place), or elsewhere that include learners will be selected carefully and will comply with good practice guidance on the use of such images
- Learners' full names will not be used anywhere on a website or blog, particularly in association with photographs
- Written permission from parents or carers will be obtained before photographs of learners are published on the school/college website
- Learners' work can only be published with the permission of the learner and parents or carers.

Data protection

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

The school must ensure that:

- **it has a Data Protection Policy (see appendix for template policy)**
- **it implements the data protection principles and is able to demonstrate that it does so**
- **it has paid the appropriate fee to Information Commissioner's Office (ICO)**
- **it has appointed an appropriate Data Protection Officer (DPO) who has a high level of understanding of data protection law and is free from any conflict of interest**
- **it has an 'information asset register' in place and knows exactly what personal data it holds, where, why and which member of staff has responsibility for managing it**
- **the information asset register lists the lawful basis for processing personal data (including, where relevant, consent). Where special category data is processed, an additional lawful basis will have also been listed**
- **it will hold the minimum personal data necessary to enable it to perform its function and it will not hold it for longer than necessary for the purposes it was collected for. The school should develop and implement a 'retention schedule" to support this**
- **data held must be accurate and up to date where this is necessary for the purpose you hold it for. Have systems in place to identify inaccuracies, such as asking parents to check emergency contact details at suitable intervals**

- **it provides staff, parents, volunteers, teenagers and older children with information about how the school / college looks after their data and what their rights are in a clear Privacy Notice** (see Privacy Notice section in the appendix)
- **procedures must be in place to deal with the individual rights of the data subject, e.g. one of the dozen rights applicable is that of Subject Access which enables an individual to see to have a copy of the personal data held about them**
- **data Protection Impact Assessments (DPIA) are carried out where necessary. For example, to ensure protection of personal data when accessed using any remote access solutions, or entering into a relationship with a new supplier**
- IT system security is ensured and regularly checked. Patches and other security essential updates are applied promptly to protect the personal data on the systems. Administrative systems are securely ring fenced from systems accessible in the classroom/to learners
- **it has undertaken appropriate due diligence and has GDPR compliant contracts in place with any data processors**
- **it understands how to share data lawfully and safely with other relevant data controllers. In Wales, schools and colleges should consider using the Wales Accord on Sharing Personal Information toolkit to support regular data sharing between data controllers**
- **there are clear and understood policies and routines for the deletion and disposal of data**
- **it reports any relevant breaches to the Information Commissioner within 72hrs of becoming aware of the breach as required by law. It also reports relevant breaches to the individuals affected as required by law. In order to do this it has a policy for reporting, logging, managing, investigating and learning from information risk incidents.**
- **If a maintained school/college, it must have a Freedom of Information Policy which sets out how it will deal with FOI requests.**
- **all staff receive data protection training at induction and appropriate refresher training thereafter. Staff undertaking particular data protection functions, such as handling requests under the individual's rights, will receive training appropriate for their function as well as the core training provided to all staff.**

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

- **data must be encrypted and password protected**
- **device must be password protected** (be sure to select devices that can be protected in this way)
- **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 (below) once it has been transferred or its use is complete**

Staff must ensure that they:

- **at all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse**
- **can recognise a possible breach, understand the need for urgency and know who to report it to within the school**
- **can help data subjects understands their rights and know how to handle a request whether verbal or written. Know who to pass it to in the school**
- **only use encrypted mobile devices (including USBs) for personal data, particularly when it is about children**
- **will not transfer any school/college personal data to personal devices except as in line with school policy**

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

Communication technologies

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 and other adults			Learners				
	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission	Not allowed
Mobile phones may be brought to school/college		■				■		
Use of mobile phones in lessons				■				
Use of mobile phones in social time		■				■		
Taking photos on mobile phones/cameras			■	■				
Use of other mobile devices, e.g. tablets, gaming devices		■		■				
Use of personal e-mail addresses in school/college, or on school/college network		■		■				
Use of school/college e-mail for personal e-mails		■		■				
Use of messaging apps		■		■				
Use of social media		■		■				
Use of blogs		■		■				

When using communication technologies the school/college considers the following as good practice:

- **the official school e-mail service may be regarded as safe and secure and is monitored. Users should be aware that e-mail communications are monitored.** Staff and learners 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/college policy – the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication**
- **any digital communication between staff and learners or parents/carers (e-mail, chat, learning platform, etc.) must be professional in tone and content.** These communications may only take place on official (monitored) school systems. Personal e-mail addresses, text messaging or social media must not be used for these communications

- learners should be taught about online safety issues, such as the risks attached to the sharing of personal details. They should also be taught strategies to deal with inappropriate communications and be reminded of the need to communicate appropriately when using digital technologies.
- personal information should not be posted on the school
- website and only official e-mail addresses should be used to identify members of staff

Social media

With an increase in use of all types of social media for professional and personal purposes a policy that sets out clear guidance for staff to manage risk and behaviour online is essential. Core messages should include the protection of learners, the school/college and the individual when publishing any material online.

Expectations for teachers' and support staffs' professional conduct are set out in the Professional Standards documentation but all adults working with children and young people must understand that the nature and responsibilities of their work place them in a position of trust and that their conduct should reflect this.

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

The school provides the following measures to ensure reasonable steps are in place to minimise risk of harm to learners through:

- ensuring that personal information is not published
- training being provided including acceptable use, social media risks, checking of settings, data protection and reporting issues
- clear reporting guidance, including responsibilities, procedures and sanctions

School staff should ensure that:

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

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

- a process for approval by senior leaders
- clear processes for the administration and monitoring of these accounts – involving at least two members of staff
- a code of behaviour for users of the accounts
- systems for reporting and dealing with abuse and misuse
- understanding of how incidents may be dealt with under school disciplinary procedures.

Personal use

- Personal communications are those made via a personal social media accounts. In all cases, where a personal account is used which associates itself with, or impacts on, the school it must be made clear that the member of staff is not communicating on behalf of the school with an appropriate disclaimer. Such personal communications are within the scope of this policy.

- Personal communications which do not refer to or impact upon the school are outside the scope of this policy.
- Where excessive personal use of social media in school is suspected, and considered to be interfering with relevant duties, disciplinary action may be taken.
- The school permits reasonable and appropriate access to private social media sites.

Monitoring of public social media

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

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

Unsuitable/inappropriate activities

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

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

User actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Users shall not visit internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	child sexual abuse images – the making, production or distribution of indecent images of children, contrary to The Protection of Children Act 1978					X
	grooming, incitement, arrangement or facilitation of sexual acts against children Contrary to the Sexual Offences Act 2003					X
	possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character), contrary to the Criminal Justice and Immigration Act 2008					X
	criminally racist material in UK – to stir up religious hatred (or hatred on the grounds of sexual orientation) - contrary to the Public Order Act 1986					X
	pornography				X	
	promotion of any kind of discrimination				X	
	threatening behaviour, including promotion of physical violence or mental harm				X	
	promotion of extremism or terrorism				X	
	any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school/college or brings the school/college into disrepute				X	
Using school/college systems to run a private business					X	
Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school/college					X	
Infringing copyright					X	
Revealing or publicising confidential or proprietary information, (e.g.					X	

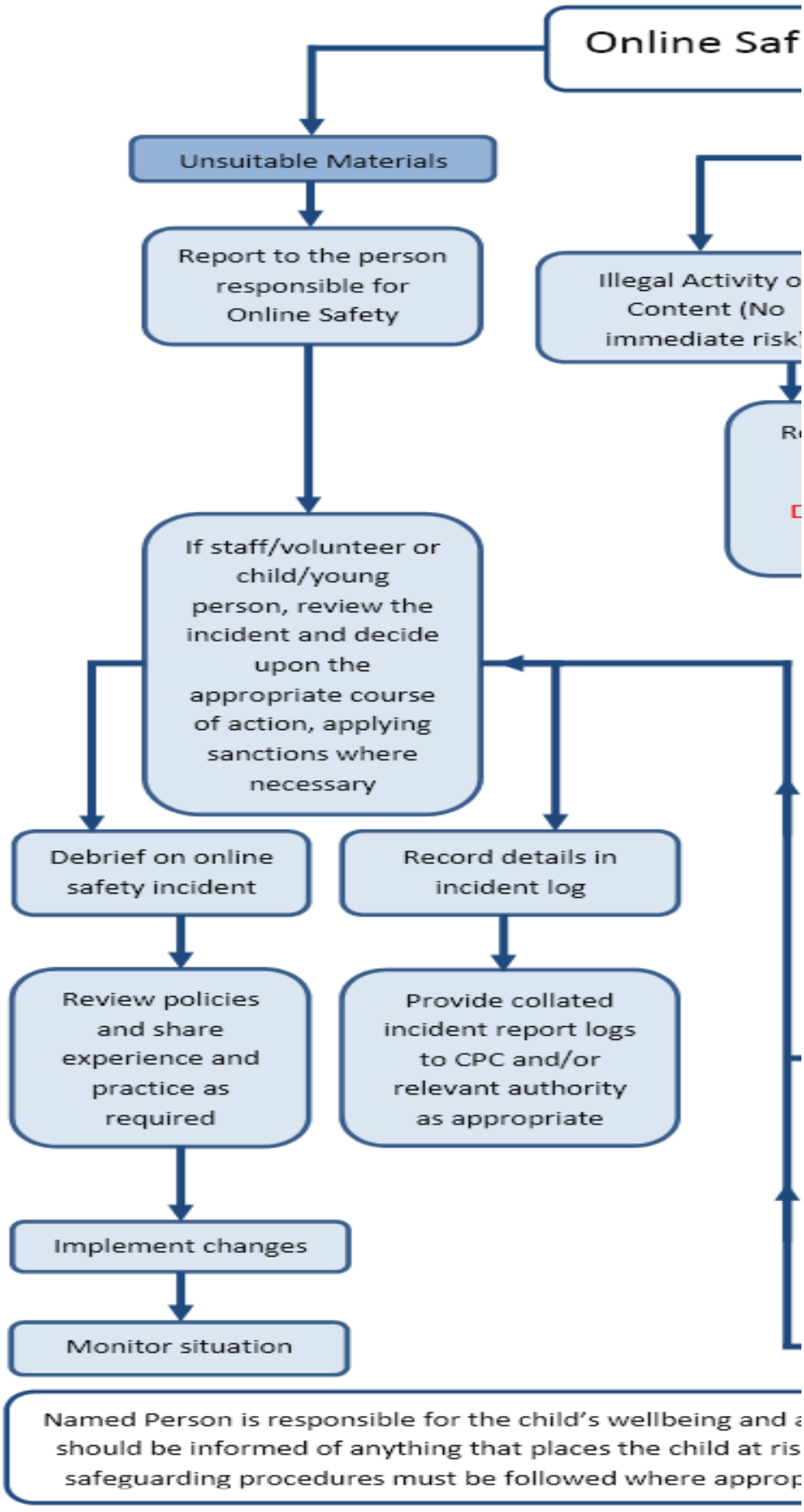
financial/personal information, databases, computer/network access codes and passwords)					
Creating or propagating computer viruses or other harmful files				X	
Unfair usage (downloading/uploading large files that hinders others in their use of the internet)				X	
Online gaming (educational)		x			
Online gaming (non educational)				x	
Online gambling				x	
Online shopping/commerce				x	
File sharing			x		
Use of social media				x	
Use of messaging apps				x	
Use of video broadcasting, e.g. YouTube				x	

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 website(s) concerned may contain child abuse images, or if there is any other suspected illegal activity, refer to the right hand side of the flowchart (below and appendix) for responding to online safety incidents and report immediately to the police.


Online Saf
Unsuitable Materials
Report to the person responsible for Online Safety
Illegal Activity o
Content (No
immediate risk)
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 policies and share experience and practice as required
Provide collated incident report logs to CPC and/or relevant authority as appropriate
Implement changes
Monitor situation
Named Person is responsible for the child's wellbeing and
should be informed of anything that places the child at ris
safeguarding procedures must be followed where approp

Other incidents

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

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

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

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

School actions

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

Learner actions

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

Staff Actions

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

Appendices

1. Acceptable User Agreements (learners, staff/volunteers)
2. Incident response flowchart
3. Reporting log template
4. Record of reviewing sites prior to use or after an incident of misuse
5. Training needs audit log
6. Summary of legislation and links to other organisations and documents

Acceptable use agreement KS3 and 4

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

For my own personal safety:

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

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

- I understand that the school systems and devices are primarily intended for educational use and that I will only use them for personal or recreational use if I have permission
- I will only make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work, if I have permission
- I will not use the school systems or devices for online gaming, online gambling, internet shopping, file sharing, or video broadcasting (eg YouTube) unless there was a specific reason given by staff and if I have permission of a member of staff to do so
- I will act as I expect others to act toward me:
- I will respect others' work and property and will only access, copy, remove or alter any other user's files, with the owner's knowledge and permission
- I will be polite and responsible when I communicate with others, I will not use strong, aggressive or inappropriate language and I appreciate that others may have different opinions
- I will only take or distribute images of others with their permission.

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

- I will only use my own personal device(s) in school, if I have permission and I understand that, if I do use my own device(s) in the school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment
- I understand the risks and will not try to upload, download or access any materials which are illegal or inappropriate or may cause harm or distress to others, nor will I try to use any programmes or software that might allow me to bypass the filtering/security systems in place to prevent access to such materials
- I will immediately report any damage or faults involving equipment or software, however this may have happened
- I will only open hyperlinks in emails or attachments to emails, if I know and trust the person/organisation who sent the email, and have no concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes)
- I will only install/ store programmes on a school device, if I have permission
- I will not access or use social media sites during school hours, either on my mobile device or on a school device

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

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

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

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

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

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/college systems and devices (both in and out of school)
- I use my own devices in the school (when allowed), e.g. mobile phones, 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, learning platforms etc

Name of Learner:.....

Group/Class .....

Signed: .....

Date: .....

Parent/Carer Countersignature

……..Date:……

Acceptable use agreement staff and volunteers

School policy

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

This acceptable use agreement is intended to ensure:

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

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

Acceptable use agreement

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

For my professional and personal safety:

- I understand that the school will monitor my use of the ICT systems, email and other digital communications
- I understand that the rules set out in this agreement also apply to use of school ICT systems (e.g. laptops, email, VLE etc.) out of school 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 not use the systems for personal or recreational use
- I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may steal it
- I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person

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

- I will only access, copy, remove or alter any other user's files, with their express permission
- I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions
- I will ensure that when I take and/or publish images of others I will do so with their permission and in accordance with the school's policy on the use of digital/video images. I will only use my personal equipment to record these images, if I have permission to do so. Where these images are published, (e.g. on the school website when developed/learning platform) it will not be possible to identify by name, or other personal information, those who are featured
- I will only use chat and social networking sites in school in accordance with the school's policies eg, a learning activity on a webinar
- I will only communicate with learners and parents/carers using official school systems. Any such communication will be professional in tone and manner

- I will not engage in any online activity that may compromise my professional responsibilities

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

- When I use my mobile devices laptops/mobile phones/USB devices etc) in school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment. I will also follow any additional rules set by the school about such use. I will ensure that any such devices are protected by up to date anti-virus software and are free from viruses.
- I will not use personal email addresses on the school digital technology systems
- I will not open any hyperlinks in emails or any attachments to emails, unless the source is known and trusted, or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes)
- I will ensure that my data is regularly backed up, in accordance with relevant school policies
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, extremist material or adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering/security systems in place to prevent access to such materials
- I will only make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work, with permission
- I will not install or attempt to install/store programmes on school devices
- 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 personal data policy (or other relevant policy). Where digital personal data is transferred outside the secure local network, it must be encrypted. Paper based protected and restricted data must be held in lockable storage
- I understand that data protection policy requires that any staff or learner data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by school policy to disclose such information to an appropriate authority
- I will immediately report any damage or faults involving equipment or software, however this may have happened

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

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

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

- I understand that this acceptable use agreement 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 as per the Disciplinary Policy 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/college and when carrying out communications related to the school/college) within these guidelines.

Staff/Volunteer Name: .....

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

Digital images and videos

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

Images may also be used to celebrate success through their publication in newsletters, on the school website and occasionally in the public media. Where an image is publically shared by any means, only your child's first name/initials will be used.

The school will comply with data protection legislation and request parents/carers permission before taking images of members of the school.

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 learners in the digital / video images.

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

Digital/Video Images Permission Form

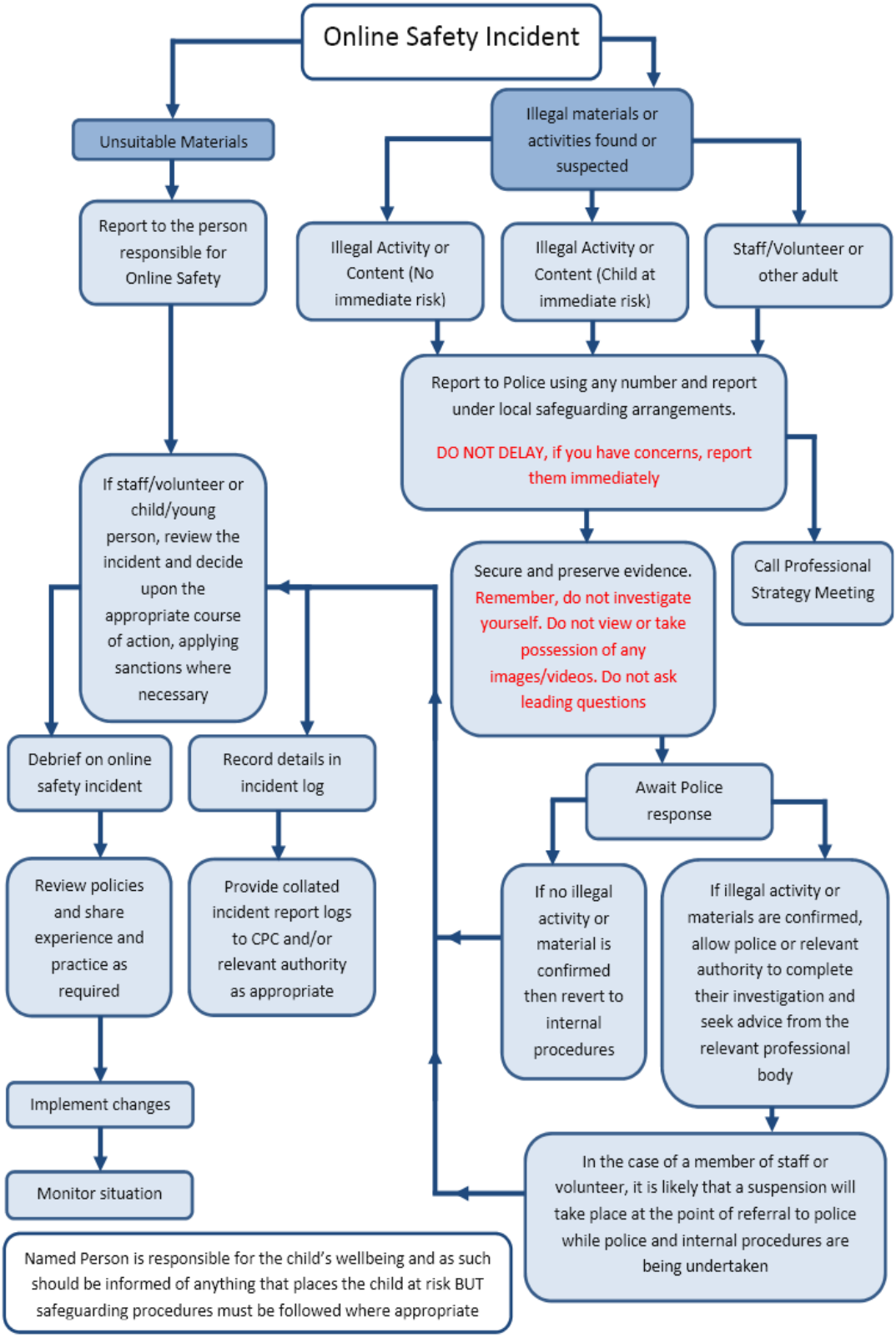
Parent/Carers Name: .....

Learner Name(s): .....

As the parent /carer of the above learner, I agree to the school taking digital/video images of my child/children.	Yes / No
I agree to these images being used:	
• to support learning activities within school	Yes / No
• in publicity that reasonably celebrates success and promotes the work of the school	Yes / No
• on a school website (under development) or other social media eg .tiwtter	Yes / No
I agree that if I take digital or video images at, or of – school /college events which include images of children other than my own, I will abide by these guidelines in my use of these images.	Yes / No

Signed:……Date:……

C1 Responding to incidents of misuse – flow chart



Record of reviewing devices/internet sites

(responding to incidents of misuse)

Group	
Date	
Reason for investigation	

Details of first reviewing person

Name	
Position	
Signature	

Details of second reviewing person

Name	
Position	
Signature	

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

Web site(s) address/device Reason for concern

Conclusion and action proposed or taken

Reporting Log

Maintained by Head/Safeguarding Officer/Deputy Safeguarding Officer

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

Training Needs Audit Log Template

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

C5 Summary of Legislation

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

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

Computer Misuse Act 1990

This Act makes it an offence to:

- erase or amend data or programs without authority;
- obtain unauthorised access to a computer;
- "eavesdrop" on a computer;
- make unauthorised use of computer time or facilities;
- maliciously corrupt or erase data or programs;
- deny access to authorised users.

Data Protection Act 2018

Controls how personal information is used by organisations, businesses or the government. The Data Protection Act 2018 is the UK's implementation of the General Data Protection Regulation (GDPR).

Everyone responsible for using personal data has to follow strict rules called 'data protection principles'. They must make sure the information is:

- used fairly, lawfully and transparently
- used for specified, explicit purposes
- used in a way that is adequate, relevant and limited to only what is necessary
- accurate and, where necessary, kept up to date
- kept for no longer than is necessary
- handled in a way that ensures appropriate security, including protection against unlawful or unauthorised processing, access, loss, destruction or damage

There is stronger legal protection for more sensitive information, such as:

- race
- ethnic background
- political opinions
- religious beliefs
- trade union membership
- genetics
- biometrics (where used for identification)
- health
- sex life or orientation

Your rights

Under the Data Protection Act 2018, you have the right to find out what information the government and other organisations store about you. These include the right to:

- be informed about how your data is being used
- access personal data
- have incorrect data updated
- have data erased
- stop or restrict the processing of your data
- data portability (allowing you to get and reuse your data for different services)
- object to how your data is processed in certain circumstances

You also have rights when an organisation is using your personal data for:

- automated decision-making processes (without human involvement)
- profiling, for example to predict your behaviour or interests

Freedom of Information Act 2000

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

Communications Act 2003

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

Malicious Communications Act 1988

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

Regulation of Investigatory Powers Act 2000

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

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

Trade Marks Act 1994

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

Copyright, Designs and Patents Act 1988

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

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

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

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

Racial and Religious Hatred Act 2006/Public Order Act 1986

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

Protection from Harrassment 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 a anyone under the age of 18.. An image of a child also covers pseudo-photographs (digitally collated or otherwise). A person convicted of such an offence is liable to imprisonment for a term of not more than 10 years, or to a fine or to both.

Sexual Offences Act 2003

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

Public Order Act 1986

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

Obscene Publications Act 1959 and 1964

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

Human Rights Act 1998

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

- the right to a fair trial
- the right to respect for private and family life, home and correspondence
- freedom of thought, conscience and religion

- freedom of expression
- freedom of assembly
- prohibition of discrimination
- the right to education
- the right not to be subjected to inhuman or degrading treatment or punishment

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

The Protection of Freedoms Act 2012

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

The Counter-Terrorism and Security Act 2015

Places a responsibility on schools to participate in work to prevent people from being drawn into terrorism, and challenge extremist ideas that support or are shared by terrorist groups.

C6 Links to other organisations or documents

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

Welsh Government

- National Online Safety Plan for children and young people in Wales – July 2018
- Welsh Government - Respect and Resilience - Community Cohesion - Guidance and associated tool to support the development of community cohesion and prevent extremism in schools and other educational settings in Wales.

UK Safer Internet Centre

- Safer Internet Centre
- South West Grid for Learning
- Childnet
- Professionals Online Safety Helpline
- Internet Watch Foundation

CEOP

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

Others

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

Cyberbullying

- Welsh Government – Anti Bullying Guidance
- Scottish Anti-Bullying Service, Respectme - http://www.respectme.org.uk/
- Scottish Government - Better relationships, better learning, better behaviour

- Anti-Bullying Network - http://www.antibullying.net/cyberbullying1.htm
- Cyberbullying.org - http://www.cyberbullying.org/
- Enable – EU funded anti-bullying project - http://enable.eun.org/

Sexting

- UKCCIS - Sexting in schools and colleges (available in English and Welsh)
- UKSIC – Responding to and managing sexting incidents

Social Networking

- Digizen – Social Networking
- Connectsafely Parents Guide to Facebook
- UKSIC – Social Media Guides

Curriculum

- Welsh Government – Digital Competence Framework
- DCF Professional Learning Needs Tool
- SWGfL Online Safety Resource (accessed through Hwb)
- UKCCIS – Education for a Connected World- Framework
- Teach Today – www.teachtoday.eu/
- Insafe - Education Resources

Mobile Devices/BYOD

Cloudlearn Report Effective practice for schools moving to end locking and blocking

NEN - Guidance Note - BYOD

Data Protection

Welsh Government - Information, guidance and templates to support schools in the implementation of our information management strategy (IMS) and to ensure biometric data is properly collected and processed.

- Information Commissioners Office:
  - ICO Guide for Organisations (general information about Data Protection)
  - ICO Guides for Education (wide range of sector specific guides)
  - DfE advice on Cloud software services and the Data Protection Act
  - ICO Guidance on Bring Your Own Device
  - ICO Guidance on Cloud Computing
  - ICO - Guidance we gave to schools - September 2012
  - 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

- **General Teaching Council for Wales - The Code of Professional Conduct and Practice**
- Kent - Safer Practice with Technology
- Childnet/TDA - Social Networking - a guide for trainee teachers & NQTs
- Childnet/TDA - Teachers and Technology - a checklist for trainee teachers & NQTs
- UK Safer Internet Centre Professionals Online Safety Helpline

Infrastructure/Technical Support

- Somerset - Questions for Technical Support
- NEN - Guidance Notes

Working with parents and carers

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

C7 Glossary of terms

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

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

Every reasonable effort has been made to ensure that the information included in this template is accurate, as at the date of publication in October 2018. 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/college conduct or discipline.