Maindee Primary

Online Safety Policy

Date Agreed	Review Date	Person Responsible
November 2015	November 2016	EN/SD/Governor Committee
November 2019	June 2020	JC/SG/Governor Committee
November 2021		MS/DJ/JR

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

Development / Monitoring / Review of this Policy

This Online Safety policy has been developed by the Digital Curriculum Team made up of:

- Headteacher / DHT
- Digital Leader
- Online Safety lead
- Staff
- Governors
- Parents
- Learners

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 *Governing Body / on:*	
The implementation of this Online Safety policy will be monitored by the:	DHT Digital Leader E- Safety Lead E- Safety Pupil Group Digital leader pupil group
Monitoring will take place at regular intervals:	Every May ready for new academic year or if necessary
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:	Twice annually (April & October)
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:	May 2022
Should serious Online Safety incidents take place, the following external persons / agencies should be informed:	LA Safeguarding Officer Police

The school will monitor the impact of the policy using:

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

Roles and Responsibilities

The following section outlines the Online Safety roles and responsibilities of individuals and groups within the school:

Governors:

Governors are responsible for the approval of the policy and for reviewing the effectiveness of the policy. This will be carried out by the Governing body receiving regular information about Online Safety incidents and monitoring reports. A member of the Governing Body has taken on the role responsible for Online Safety which includes:

- meetings with the Online Safety lead
- regular monitoring of Online Safety incident logs
- regular monitoring of filtering / change control logs
- reporting to relevant Governors

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 is delegated to the Digital Leader (Mr Dale Jones).
- The Headteacher and another member of the Senior Leadership Team / Senior Management Team are 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 and Online Safety Coordinator are responsible for ensuring that the Online Safety Coordinator 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 will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal Online Safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.
- The Senior Leadership Team will receive regular monitoring reports from the Online Safety Coordinator.

Online Safety Lead:

The Online Safety Lead

- liaises with the teacher (Mr Jonathon Rowe) of the Online Safety group
- takes day to day responsibility for Online Safety issues and has a leading role in establishing and reviewing the school Online Safety policies / documents along with the digital leader
- 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 technical staff
- receives reports of Online Safety incidents and creates a log of incidents to inform future Online Safety developments.
- meets with Online Safety Governor to discuss current issues, review incident logs and if possible, filtering / change control logs
- attends relevant meetings, including regular EAS Digital Network meetings and Newport schools digital network meetings
- reports regularly to Senior Leadership Team
- Hosts digital safety workshops for parents when necessary

Technical support:

The *Deputy Headteacher* 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 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 is applied and updated on a regular basis and its implementation is not the sole responsibility of any single person* (see appendix "Technical Security Policy Template" for good practice)
- 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 / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the Headteacher / Online Safety Coordinator for investigation / action / sanction
- that monitoring software / systems are implemented and updated as agreed in school policies

Teaching and Support Staff

Are responsible for ensuring that:

- they have an up to date awareness of Online Safety matters and of the current school Online Safety policy and practices
- they have read, understood and signed the Staff Acceptable Use Agreement (AUA)
- they report any suspected misuse or problem to the *Headteacher / Online Safety Coordinator* for investigation / action
- all digital communications with students / learners / parents / carers should be on a professional level
- 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

Safeguarding Designated Person

The Safeguarding Officer should be trained in Online Safety issues and be aware of the potential for serious safeguarding issues to arise from:

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

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 monitoring the Online Safety policy including the impact of initiatives. The group will also be responsible for regular reporting to the Governing Body.

Members of the Online Safety Group will assist the Online Safety Coordinator with:

- the production / review / monitoring of the school Online Safety policy / documents.
- the production / review / monitoring of the school filtering policy and requests for filtering changes.
- mapping and reviewing the Online Safety curricular provision – ensuring relevance, breadth and progression
- monitoring network / internet / incident logs where possible

- consulting stakeholders – including parents / carers and the students / learners about the Online Safety provision
- monitoring improvement actions identified through use of the 360 degree safe Cymru self review tool

Students / learners:

- 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 cyber-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,website (HWB), social media, National and local Online Safety campaigns and 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
- Learner platforms such as seesaw, google classroom and HWB

Community Users

No community user access at the school.

Policy Statements

Education – learners

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

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

- **A planned Online Safety curriculum across a range of subjects (e.g. ICT/PSE/DCF) and topic areas and regularly revisited**
- **Key Online Safety messages should be reinforced as part of a planned programme of assemblies and activities**
- **Learners 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.**
- **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 design making.**
- learners should be helped to understand the need for the pupil Acceptable Use Agreement and encouraged to adopt safe and responsible use both within and outside 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.

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 platforms , HWB
- Parents / Carers workshops
- High profile events / campaigns eg Safer Internet Day
- Reference to the relevant web sites / publications eg https://hwb.wales.gov.uk/ www.saferinternet.org.uk/ http://www.childnet.com/parents-and-carers

Education – The Wider Community

The school will provide opportunities for local community groups / members of the community to gain from the school'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.
- Learning platforms / HWB website
- The school website will provide Online Safety information for the wider community

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.**
- The Online Safety Coordinator (or other nominated person) will receive regular updates through attendance at external training events (eg from Consortium / SWGfL / LA / other relevant organisations) and by reviewing guidance documents released by relevant organisations.
- This Online Safety policy and its updates will be presented to and discussed by staff in staff / phase meetings.
- The Online Safety Coordinator (or other nominated person) will provide advice / guidance / training to individuals as required.

Training – Governors

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

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

Technical – infrastructure / equipment, filtering and monitoring

The school will be responsible for ensuring that the school infrastructure / network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also 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 Upper and Lower Phase users will be provided with a username and secure password** by the 21st Century Learning Leader who will keep an up to date record of users and their usernames. **Year 5 & 6 learners are responsible for the security of their username and password**.
- **The "master / administrator" passwords for the school ICT system, 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.**
- **21st Century Learning Leader 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.
- 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.
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, mobile devices etc from accidental or malicious attempts which might threaten the security of the school systems and data. These are tested regularly.
- An agreed policy of issuing a temporary login is in place for the provision of temporary access of "guests" (eg trainee teachers, supply teachers, visitors) onto the school systems.
- An agreed policy is in place regarding the extent of personal use that users (staff / students / learners / community users) and their family members are allowed on school devices that may be used out of school.
- An agreed policy is in place that allows staff to / forbids staff from downloading executable files and installing programmes on school devices.
- An agreed policy is in place regarding the use of removable media (eg memory sticks / CDs / DVDs) by users on school devices. Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured.

Use of digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and learners instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents / carers and students / learners need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for cyberbullying to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. It is common for employers to carry out internet searches for information about potential and existing employees. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- **When using digital images, staff should inform and educate learners about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet eg on social networking sites.**
- In accordance with guidance from the Information Commissioner's Office, parents / carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use in not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published /

made publicly available on social networking sites, nor should parents / carers comment on any activities involving other learners in the digital / video images.

- Staff and volunteers are allowed to take digital / video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment, if they have to be taken on personal equipment then they will be deleted immediately after use.
- Care should be taken when taking digital / video images that learners are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- learners must not take, use, share, publish or distribute images of others without their permission
- Photographs published on the website, or elsewhere that include learners will be selected carefully and will comply with good practice guidance on the use of such images.
- learners' full names will not be used anywhere on a website or blogs, particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs of learners are published on the school website
- Pupil's work can only be published with the permission of the pupil and parents or carers.

Data Protection

Personal data will be recorded, processed, transferred and made available according to the 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 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. The school may also wish to appoint a Data Manager and Systems Controllers to support the DPO
- 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 Online safety policy template for schools and colleges 16
- 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, it must have a Freedom of Information Policy which sets out how it will deal with FOI requests. • all staff receive data protection training at induction and appropriate refresher training thereafter. Staff undertaking particular data protection functions, such as handling requests under the individual's rights, will receive training appropriate for their function as well as the core training provided to all staff.

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

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

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

- the official school e-mail service (HWB) 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 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
- whole class/group e-mail addresses may be used at Foundation Stage , while learners at Key Stage 2 and above will be provided with individual school e-mail (HWB) addresses for educational use.
- 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 - Protecting Professional Identity

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

Expectations for teachers' professional conduct are set out by the General Teaching Council Wales (GTCW) but all adults working with children and young people must understand that the nature and responsibilities of their work place them in a position of trust and that their conduct should reflect this.

All schools 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, cyberbully, discriminate on the grounds of sex, race or disability or who defame a third party may render the school or local authority liable to the injured party. Reasonable steps to prevent predictable harm must be in place. All staff working at any educational establishment are expected to demonstrate a professional approach and respect for learners and their families and for colleagues and the learning setting.

The school provides the following measures to ensure reasonable steps are in place to minimise risk of harm to 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
- risk assessment, including legal risk.

School staff should ensure that:

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

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

- a process for approval by senior leaders
- clear processes for the administration and monitoring of these accounts – involving at least two members of staff
- a code of behaviour for users of the accounts
- 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

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					
	promotion of any kind of discrimination					
	threatening behaviour, including promotion of physical violence or mental harm					
	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					
Using school systems to run a private business						
Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school						
Infringing copyright						
Revealing or publicising confidential or proprietary information (eg financial / personal information, databases, computer / network access codes and passwords)						
Creating or propagating computer viruses or other harmful files						
Unfair usage (downloading / uploading large files that hinders others in their use of the internet)						
On-line gaming (educational)						
On-line gaming (non educational)						

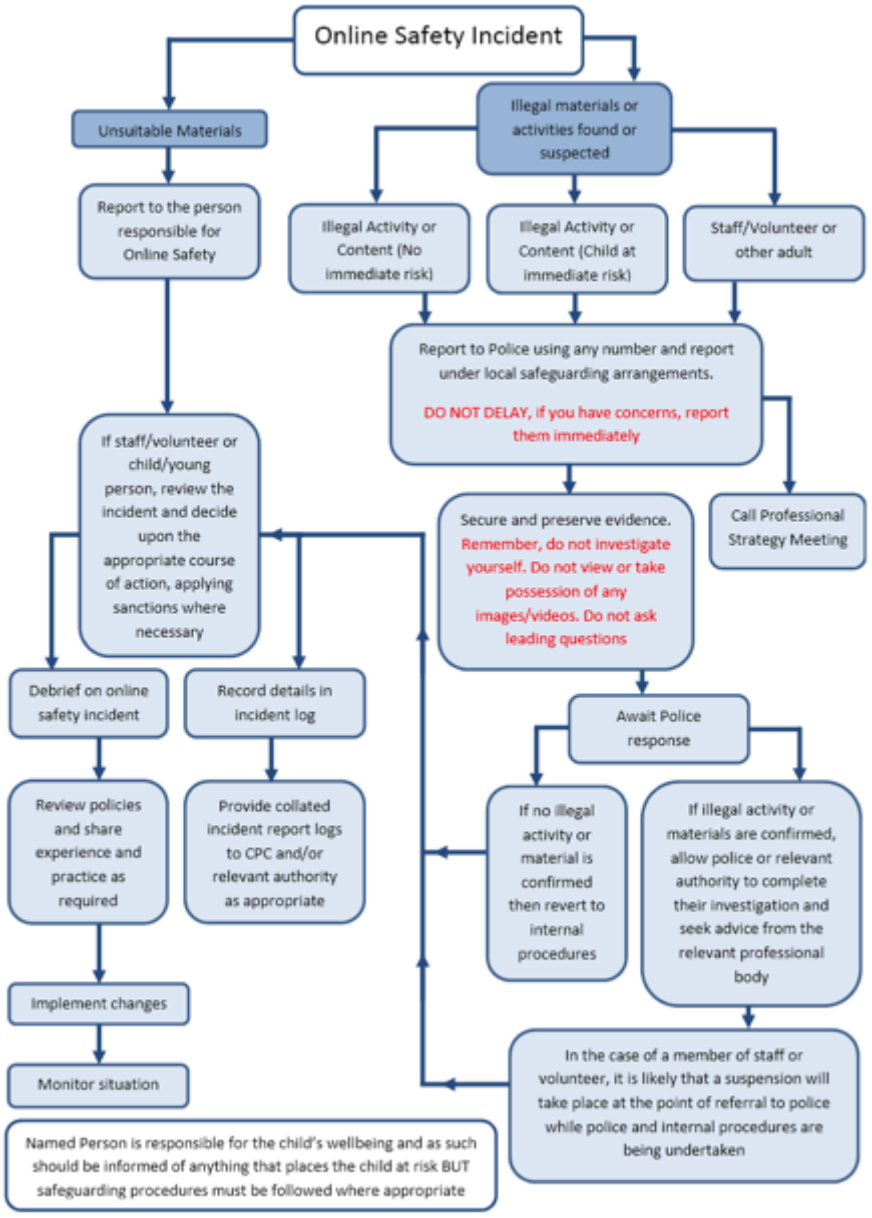
On-line gambling					
On-line shopping / commerce			X		
File sharing			X		
Use of social media			x		
Use of messaging apps					
Use of video broadcasting eg Youtube					

Responding to incidents of misuse

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

Illegal Incidents

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



Other Incidents

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

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

- Have more than one senior member of staff / volunteer involved in this process. This is vital to protect individuals if accusations are subsequently reported.
- Conduct the procedure using a designated computer that will not be used by young people and if necessary can be taken off site by the police should the need arise. Use the same computer for the duration of the procedure.

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

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

School actions

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

Pupils

Incidents	Warning	Restorative conversation at Break / Lunch time	HT / DHT / Phase Leader	Police	Technical support	Inform parents / carers	Removal of internet / Device break	Exclusion
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).		/	/			/		
Unauthorised use of non-educational sites during lessons	/							
Unauthorised use of mobile phone / digital camera / other mobile device			/			/		

Unauthorised use of social media / messaging apps / personal email			/			/		
Unauthorised downloading or uploading of files		/						
Allowing others to access school network by sharing username and passwords		/				/		
Attempting to access or accessing the school network, using another student's / pupil's account	/							
Attempting to access or accessing the school network, using the account of a member of staff			/			/		
Corrupting or destroying the data of other users							/	
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature		/				/		
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school		/						
Using proxy sites or other means to subvert the school's 's filtering system		/				/		
Accidentally accessing offensive or pornographic material and failing to report the incident		/				/		
Deliberately accessing or trying to access offensive or pornographic material			/			/	/	
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act	/	/						
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).						/		
Inappropriate personal use of the internet / social media / personal email		/	/			/		
Careless use of personal data eg holding or transferring data in an insecure manner	/							
Deliberate actions to breach data protection or network security rules		/						
Corrupting or destroying the data of other users or causing deliberate			/			/	/	

damage to hardware or software								
Actions which could compromise the staff member's professional standing			/			/	/	
Breaching copyright or licensing regulations	/							
Continued infringements of the above, following previous warnings or sanctions			/			/	/	

Staff

Incidents	HT / DHT	LA / HR	Police	Technical Support	Warning	Suspension	Disciplinary
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).	/	/	/				
Unauthorised use of non-educational sites during lessons	/						
Unauthorised use of mobile phone / digital camera / other mobile device	/						
Unauthorised use of social media / messaging apps / personal email	/						
Unauthorised downloading or uploading of files	/						
Allowing others to access school network by sharing username and passwords	/			/			
Attempting to access or accessing the school network, using the account of a member of staff	/				/		
Corrupting or destroying the data of other users	/				/	/	/
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature	/	/			/		

Actions which could bring the school into disrepute or breach the integrity of the ethos of the school	/						
Using proxy sites or other means to subvert the school's 's filtering system	/			/	/		
Accidentally accessing offensive or pornographic material and failing to report the incident	/			/			
Deliberately accessing or trying to access offensive or pornographic material	/	/	/	/	/	/	/
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act	/			/			
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).	/	/	/	/	/	/	/
Inappropriate personal use of the internet / social media / personal email	/						
Careless use of personal data eg holding or transferring data in an insecure manner	/			/			
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software	/			/	/	/	/
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature	/	/		/	/	/	/
Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with students / pupils	/	/	/	/	/	/	/
Breaching copyright or licensing regulations	/				/		
Continued infringements of the above, following previous warnings or sanctions	/	/	/	/	/	/	/

A1 Pupil Acceptable Use Agreement – Foundation Phase

This is how we stay safe when we use computers:

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

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

⬚ I will take care of the computer and other equipment

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

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

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

Signed (on behalf of the child):……

Signed (parent): ……..

A2 Pupil Acceptable Use Agreement (AUA) – KS2

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

This Acceptable Use Agreement is intended to ensure:

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

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

Acceptable Use Agreement

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

For my own personal safety:

- I understand that the school will monitor my use of IT systems, devices and digital communications.
- I will keep my username and password safe and secure – I will not share it, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may steal it.
- I will be aware of "stranger danger", when I am communicating online.
- 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 offline 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 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 not use them for personal or recreational use unless I have permission.
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not use the school systems or devices for on-line gaming, on-line gambling, internet shopping, file sharing, or video broadcasting (eg YouTube), unless I have permission of a member of staff to do so.

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

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

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

- I will only use my own personal device(s) in school if I have permission. I understand that, if I do use my own device(s) in the school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment.
- I understand the risks and will not try to upload, download or access any materials which are illegal or inappropriate or may cause harm or distress to others, nor will I try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.

- I will not open any hyperlinks in emails or any attachments to emails, unless I know and trust the person / organisation who sent the email, or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes)
- I will not install or attempt to install or store programmes of any type on any school device, nor will I try to alter computer settings.
- I will only use social media sites with permission and at the times that are allowed.

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

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

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

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

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

Student / Pupil Acceptable Use Agreement Form

This form relates to the 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 ICT 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) eg mobile phones, gaming devices, cameras etc
- I use my own equipment out of the school in a way that is related to me being a member of this *school* e.g. communicating with other members of the school, accessing school email, VLE, website etc.

Name of Student / Pupil	
Group / Class	
Signed	
Date	

A3 Staff (and Volunteer) Acceptable Use Agreement

School Policy

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

This Acceptable Use Policy is intended to ensure:

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

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

Acceptable Use Policy Agreement

I understand that I must use school ICT systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the ICT systems and other users. I recognise the value of the use of ICT for enhancing learning and will ensure that students / learners receive opportunities to gain from the use of ICT. I will, where possible, educate the young people in my care in the safe use of ICT and embed 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 (eg chromebooks, iPads, email) out of school, and to the transfer of personal data (digital or paper based) out of school
- I understand that the school ICT systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within the policies and rules set down by the school.
- I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may steal it.
- I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person.

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

- I will not access, copy, remove or otherwise alter any other user's files, without their express permission.
- I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will ensure that when I take and / or publish images of others I will do so with their permission and in accordance with the school's policy on the use of digital / video images. I will not use my personal equipment to record these images, unless I have no other alternative at the time. Where these images are published (eg on the school website) 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.
- Any communication with learners parents / carers will be professional in tone and manner and only with the school email address I have been issued with.
- 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 (laptops / mobile phones / USB devices etc) in school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment. I will also follow any additional rules set by the school about such use. I will ensure that any such devices are protected by up to date anti-virus software and are free from viruses.
- I will not open any hyperlinks in emails or any attachments to emails, unless the source is known and trusted , or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes)
- I will ensure that my data is regularly backed up, in accordance with relevant school policies.
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings, unless this is allowed in school policies.
- I will not disable or cause any damage to school equipment, or the equipment belonging to others.
- I will only transport, hold, disclose or share personal information about myself or others, as outlined in the School / LA Personal Data Policy (or other relevant policy). Where digital personal data is transferred outside the secure local network, it must be encrypted. Paper based Protected and Restricted data must be held in lockable storage.
- I understand that data protection policy requires that any staff or pupil data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by school policy to disclose such information to an appropriate authority.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.

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

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

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

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

Signed: Date:

A4 Parent / Carer Acceptable Use Agreement

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

This Acceptable Use Policy is intended to ensure:

- that young people will be responsible users and stay safe while using the internet and other 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 parents and carers are aware of the importance of Online Safety and are involved in the education and guidance of young people with regard to their on-line behaviour.

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

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

Permission Form

Parent / Carers Name Student / Pupil Name

As the parent / carer of the above learners, I give permission for my son / daughter to have access to the internet and to ICT systems at school.

Either: (KS2)

I know that my son / daughter has signed an Acceptable Use Agreement and has received, or will receive, Online Safety education to help them understand the importance of safe use of technology and the internet – both in and out of school.

Or: (FP)

I understand that the school has discussed the Acceptable Use Agreement with my son / daughter and that they have received, or will receive, Online Safety education to help them understand the importance of safe use of technology and the internet – both in and out of school.

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

I understand that my son's / daughter's activity on the ICT systems will be monitored and that the school will contact me if they have concerns about any possible breaches of the Acceptable Use Agreement.

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

Signed Date

B2 school personal data advice and guidance

Suggestions for use

This document is for advice and guidance purposes only. It is anticipated that schools / colleges will use this advice alongside their own data protection policy. This document is not intended to provide legal advice and the school is encouraged to seek their own legal counsel when considering their management of personal data.

The template uses the terms learners to refer to the children or young people at the institution.

school personal data handling

Recent publicity about data breaches suffered by organisations and individuals continues to make the area of personal data protection a current and high profile issue for schools, colleges and other organisations. It is important that the school has a clear and well understood personal data handling policy in order to minimise the risk of personal data breaches. A breach may arise from a theft, a deliberate attack on your systems, the unauthorised or malicious use of personal data by a member of staff, accidental loss, or equipment failure. In addition:

● no school or individual would want to be the cause of a data breach, particularly as the impact of data loss on individuals can be severe, put individuals at risk and affect personal, professional or organisational reputation

● schools/colleges are "data rich" and the introduction of electronic storage and transmission of data has created additional potential for the loss of data

● the school will want to avoid the criticism and negative publicity that could be generated by any personal data breach

● the school is subject to a wide range of legislation related to data protection and data use, with significant penalties for failure to observe the relevant legislation

● it is a legal requirement for all schools / colleges to have a Data Protection Policy and be able to demonstrate compliance with data protection law.

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

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

Introduction

Schools / Colleges and their employees must do everything within their power to ensure the safety and security of any material of a personal or sensitive nature, including personal data.

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

● have permission to access that data

● need to have access to that data.

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

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

Legislative Context

With effect from 25th May 2018, the data protection arrangements for the UK changed following the implementation of the European Union General Data Protection Regulation (GDPR). This represents a significant shift in legislation and in conjunction with the Data Protection Act 2018 replaces the Data Protection Act 1998. These two documents are intended to be read side-by-side.

The GDPR provides the principles and rights which apply across the European Union. The Data Protection Act 2018 covers the areas outside of the EU GDPR and provides the UK-specific details such as; how to handle education and safeguarding information.

Are schools / colleges in Wales required to comply?

In short, yes. Any natural or legal person, public authority, agency or other body which processes personal data is considered a 'data controller'. Given the nature of schools / colleges and the personal data required in a variety of forms to operate a school this means that all educational establishments in the UK are required to comply. Guidance for schools / colleges is available on the Information Commissioner's Office website including information about the new regulations.

Personal Data

The school / college and its employees will have access to a wide range of personal information and data. The data may be held in a digital format or on paper records. Personal data is information that relates to an identified or identifiable living individual This will include:

● personal information about members of the school community – including learners, members of staff and parents/carers e.g. names, addresses, contact details, legal guardianship contact details, health records, disciplinary records

● curricular / academic data e.g. class lists, learner progress records, reports, references

● professional records e.g. employment history, taxation and national insurance records, appraisal records and references

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

Special categories of personal data The following is a list of personal data listed in the GDPR as a 'special category'.

"revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation" In order to lawfully process special category data, you must identify both a lawful basis and a separate condition for processing special category data. You should decide and document this before you start processing the data.

Consent

Consent (which is one of the lawful bases to use data) under the regulation has changed. Consent is defined as:

"in relation to the processing of personal data relating to an individual, means a freely given, specific, informed and unambiguous indication of the individual's wishes by which the individual, by a statement or by a clear affirmative action, signifies agreement to the processing of the personal data"

This means that where a school is relying on consent as the basis for processing personal data that consent has to be clear, meaning that pre-ticked boxes, opt-out or implied consent are no longer suitable. The GDPR does not specify an age of consent for general processing but schools / colleges should consider the capacity of pupils to freely give their informed consent. The Information Commissioner's Office (ICO) gives clear advice on when it's appropriate to use consent as a lawful base. It states:

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

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

– consent would be appropriate for considering whether a child's photo could be published in any way.

– if your school or college requires learner details to be stored in an MIS, it would not be appropriate to rely on consent if the learner cannot opt out of this. In this case, you could apply the public task lawful base. Consent is just one of the six lawful bases for processing data:

1. Consent

2. Contract: the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract

3. Legal obligation: the processing is necessary for you to comply with the law

4. Vital interests: the processing is necessary to protect someone's life

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

6. Legitimate interests: processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child. (This cannot apply if you are a public authority processing data to perform your official tasks).

Previously maintained schools / colleges were able to rely on the 'legitimate interests' justification. But under the new laws, this has been removed for Public Bodies (which includes schools /colleges). However, public

bodies should consider using the Public Task lawful base whenever they are undertaking a task that is part of their statutory function.

Data Protection Impact Assessments (DPIA)

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

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

The risk assessment will involve:

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

According to the ICO a DPIA should contain:

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

Or more simply and fully:

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

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

Secure storage of and access to data

The school should ensure that systems are set up so that the existence of protected files is hidden from unauthorised users and that users will be assigned a clearance that will determine which files are accessible to them. Access to protected data will be controlled according to the role of the user. Members of staff will not, as a matter of course, be granted access to the whole management information system. Good practice suggests that all users will use strong passwords made up from a combination of simpler words. User passwords must never be shared.

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

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

Personal data should only be stored on school equipment. Private equipment (i.e. owned by the users) must not be used for the storage of school personal data.

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

● The data must be encrypted and password protected

● The device must be password protected

● The device must offer approved virus and malware checking software

● The data must be securely deleted from the device, in line with school policy once it has been transferred or its use is complete.

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

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

The school should have clear policy and procedures for the use of "Cloud Based Storage Systems" (for example Dropbox, Microsoft 365, Google Drive) and is aware that data held in remote and cloud storage is still required to be protected in line with the Data Protection Act. The school will ensure that it is satisfied with controls put in place by remote / cloud based data services providers to protect the data.

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

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

Secure transfer of data and access out of school

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

● Users may not remove or copy sensitive or restricted or protected personal data from the school or authorised premises without permission and unless the media is encrypted and password protected and is transported securely for storage in a secure location

● Users must take particular care that computers or removable devices which contain personal data must not be accessed by other users (e.g. family members) when out of school

● When restricted or protected personal data is required by an authorised user from outside the organisation's premises (for example, by a member of staff to work from their home), they should preferably have secure remote access to the management information system or learning platform

● If secure remote access is not possible, users must only remove or copy personal or sensitive data from the organisation or authorised premises if the storage media, portable or mobile device is encrypted and is transported securely for storage in a secure location

● Users must protect all portable and mobile devices, including media, used to store and transmit personal information using approved encryption software

● Particular care should be taken if data is taken or transferred to another country, particularly outside Europe, and advice should be taken from the local authority (if relevant) in this event.

Disposal of data

The school should implement a document retention schedule that defines the length of time data is held before secure destruction. The Information and Records Management Society Toolkit for schools provides support for this process. The school must ensure the safe destruction of personal data when it is no longer required.

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

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

Audit Logging / Reporting / Incident Handling

In the GDPR, organisations are required to keep records of processing activity. This must include:

● the name and contact details of the data controller

● where applicable, the name and contact details of the joint controller and data protection officer

● the purpose of the processing

● to whom the data has been/will be disclosed

● description of data subject and personal data

● where relevant the countries it has been transferred to

● under which condition for processing the data has been collected

● under what lawful basis processing is being carried out

● where necessary, how it is retained and destroyed

● a general description of the technical and organisational security measures.

Clearly, in order to maintain these records good auditing processes must be followed, both at the start of the exercise and on-going throughout the lifetime of the requirement. Therefore, audit logs will need to be kept to:

● provide evidence of the processing activity and the DPIA

● record where, how and to whom data has been shared

● log the disposal and destruction of the data

● enable the school to target training at the most at-risk data

● record any breaches that impact on the data

Data Breaches

From 25 May 2018, if you experience a personal data breach you need to consider whether this poses a risk to people. You need to consider the likelihood and severity of any risk to people's rights and freedoms, following the breach. When you've made this assessment, if it's likely there will be a risk then you must notify the ICO; if it's unlikely then you don't have to report it. You do not need to report every breach to the ICO.

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

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

● "responsible person" for each incident

● communications plan, including escalation procedure

● plan of action for rapid resolution

● plan of action of non-recurrence and further awareness raising

All significant data protection incidents must be reported through the DPO to the Information Commissioner's Office based upon the local incident handling policy and communication plan. The new laws require that this notification should take place within 72 hours of the breach being detected, where feasible.

Data Mapping

The process of data mapping is designed to help schools / colleges identify with whom their data is being shared in order that the appropriate contractual arrangements can be implemented. If a third party is processing personal data on your behalf about your learners then this processor has obligations on behalf of the school to ensure that processing takes place in compliance with data protection laws.

Data subject's right of access

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

● to be informed – Privacy Notices

● of access – Subject Access Requests

● to rectification – correcting errors

● to erasure – deletion of data when there is no compelling reason to keep it

● to restrict processing – blocking or suppression of processing

● to portability – Unlikely to be used in a school context

● to object – objection based on grounds pertaining to their situation

● related to automated decision making, including profiling

Several of these could impact schools and colleges, such as the right of access. You need to put procedures in place to deal with Subject Access Requests. These are written or verbal requests to see all or a part of the personal data held by the Controller in connection with the individual. Controllers normally have 1 calendar month to provide the information, unless the case is unusually complex in which case an extension can be obtained.

Individuals have the right to know:

● if the Controller holds personal data about them

● a description of that data

- the purpose for which the data is processed
- the sources of that data
- to whom the data may be disclosed
- a copy of all the personal data that is held about them.

A school must not disclose

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

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

Fee

The school should pay the relevant fee to the Information Commissioner's Office (ICO).

Responsibilities

Every maintained school is required to appoint a Data Protection Officer as a core function of 'the business'

The Data Protection Officer (DPO) can be internally or externally appointed.

They must have:

- expert knowledge
- timely and proper involvement in all issues relating to data protection
- the necessary resources to fulfil the role
- access to the necessary personal data processing operations
- a direct reporting route to the highest management level

The data controller must:

- not give the DPO instructions regarding the performance of tasks
- ensure that the DPO does not perform a duty or role that would lead to a conflict of interests
- not dismiss or penalise the DPO for performing the tasks required of them

As a minimum a Data Protection Officer must:

- inform, as necessary, the controller, a processor or an employee of their obligations under the data protection laws
- provide advice on a data protection impact assessment

- co-operate with the Information Commissioner
- act as the contact point for the Information Commissioner
- monitor compliance with policies of the controller in relation to the protection of personal data
- monitor compliance by the controller with data protection laws

The school may also wish to appoint a Data Manager. Schools/colleges are encouraged to separate this role from that of Data Protection Officer, where possible. This person will keep up to date with current legislation and guidance and will:

- determine and take responsibility for the school's / college's information risk policy and risk assessment
- oversee the System Controllers

The school may also wish to appoint System Controllers for the various types of data being held (e.g. learner information / staff information / assessment data etc.). These Controllers will manage and address risks to the information and will understand:

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

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

Governors are required to comply fully with this policy in the event that they have access to personal data, when engaged in their role as a Governor (either in the school or elsewhere if on school business).

Training & awareness

All staff must receive data handling awareness / data protection training and will be made aware of their responsibilities. This should be undertaken regularly. You can do this through:

- Induction training for new staff
- Staff meetings / briefings / INSET
- Day to day support and guidance from System Controllers

Freedom of Information Act

All schools / colleges must have a Freedom of Information Policy which sets out how it will deal with FOI requests. FOI aims to increase transparency and accountability in public sector organisations as part of a healthy democratic process. Whilst FOI requests are submitted by an individual, the issue is for the school to consider whether the requested information should be released into the public domain. FOI links to data protection law whenever a request includes personal data. Good advice would encourage the school to:

- delegate to the Headteacher day-to-day responsibility for FOI policy and the provision of advice, guidance, publicity and interpretation of the school's/college's policy
- consider designating an individual with responsibility for FOI, to provide a single point of reference, coordinate FOI and related policies and procedures, take a view on possibly sensitive areas and consider what information and training staff may need

● consider arrangements for overseeing access to information and delegation to the appropriate governing body

● proactively publish information with details of how it can be accessed through a Publication Scheme (see Model Publication Scheme below) and review this annually

● ensure that a well-managed records management and information system exists in order to comply with requests

● ensure a record of refusals and reasons for refusals is kept, allowing the school to review its access policy on an annual basis

B4 Reporting Log Template

B5 Links to other organisations or documents
The following links may help those who are developing or reviewing a school Online Safety policy.

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/index.aspx

Support for Schools

- Specialist help and support - SWGfL BOOST

Cyberbullying

- Scottish Anti-Bullying Service, Respectme - http://www.respectme.org.uk/
- Scottish Government - Better relationships, better learning, better behaviour
- Welsh Government – Respecting Others
- Anti-Bullying Network - http://www.antibullying.net/cyberbullying1.htm
- Cyberbullying.org - http://www.cyberbullying.org/

Social Networking

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

Curriculum

- SWGfL Digital Literacy & Citizenship curriculum
- Alberta, Canada - digital citizenship policy development guide.pdf
- Teach Today – www.teachtoday.eu/
- Insafe - Education Resources
- Somerset - e-Sense materials for schools

Mobile Devices / BYOD

- Cloudlearn Report Effective practice for schools moving to end locking and blocking
- NEN - Guidance Note - BYOD

Data Protection

- Information Commissioner's Office:
- Your rights to your information – Resources for Schools - ICO
- ICO pages for young people
- Guide to Data Protection Act - Information Commissioners Office
- Guide to the Freedom of Information Act - Information Commissioners Office
- ICO guidance on the Freedom of Information Model Publication Scheme
- ICO Freedom of Information Model Publication Scheme Template for schools (England)
- ICO - Guidance we gave to schools - September 2012 (England)
- ICO Guidance on Bring Your Own Device
- ICO Guidance on Cloud Hosted Services

- Information Commissioners Office good practice note on taking photos in schools
- ICO Guidance Data Protection Practical Guide to IT Security
- ICO – Think Privacy Toolkit
- ICO – Personal Information Online – Code of Practice
- ICO – Access Aware Toolkit
- ICO Subject Access Code of Practice
- ICO – Guidance on Data Security Breach Management

- SWGfL - Guidance for Schools on Cloud Hosted Services
- LGfL - Data Handling Compliance Check List
- Somerset - Flowchart on Storage of Personal Data
- NEN - Guidance Note - Protecting School Data

Professional Standards / Staff Training

- DfE - Safer Working Practice for Adults who Work with Children and Young People
- Kent - Safer Practice with Technology
- Childnet / TDA - Social Networking - a guide for trainee teachers & NQTs
- Childnet / TDA - Teachers and Technology - a checklist for trainee teachers & NQTs
- UK Safer Internet Centre Professionals Online Safety Helpline

Infrastructure / Technical Support

- Somerset - Questions for Technical Support
- NEN - Guidance Note - esecurity SWGfL / Common Sense Media Digital Literacy & Citizenship Curriculum

Working with parents and carers

- SWGfL BOOST Presentations - parents presentation
- Connect Safely - a Parents Guide to Facebook
- Vodafone Digital Parents Magazine
- Childnet Webpages for Parents & Carers
- DirectGov - Internet Safety for parents
- 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
- The Cybersmile Foundation (cyberbullying) - advice for parents

Research

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

B5 Glossary of terms

AUP	Acceptable Use Policy – see templates earlier in this document
CEOP	Child Exploitation and Online Protection Centre (part of UK Police, dedicated to protecting children from sexual abuse, providers of the Think U Know programmes.
CPD	Continuous Professional Development
CYPS	Children and Young People's Services (in Local Authorities)
FOSI	Family Online Safety Institute
EA	Education Authority
ICO	Information Commissioner's Office
ICT	Information and Communications Technology
ICTMark	Quality standard for schools provided by NAACE
INSET	In Service Education and Training
IP address	The label that identifies each computer to other computers using the IP (internet protocol)

ISP Internet Service Provider
ISPA Internet Service Providers' Association
IWF Internet Watch Foundation
LA Local Authority
LAN Local Area Network
MIS Management Information System
NEN National Education Network – works with the Regional Broadband Consortia (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.
VLE Virtual Learning Environment (a software system designed to support teaching and learning in an educational setting.
WAP Wireless Application Protocol

Appendices – Section A - Acceptable Use Agreement

- A1 Pupil Acceptable Use Agreement (FP)
- A2 Pupil Acceptable Use Agreement (KS2)
- A3 Staff and Volunteers Acceptable Use Agreement
- A4 Parents / Carers Acceptable Use Agreement

Appendices – Section B – Support documents and links

- B1 Record of reviewing sites (for internet misuse)
- B2 Summary of Legislation
- B3 Google Apps for Education – further details
- B4 Links to other organisations and documents
- B5 Glossary of terms