Ribblesdale
School

A foundation for success
since 1932

Ribblesdale High School

Online Safety Policy

This policy applies to all members of the school community (including staff, pupils, volunteers, parents and carers, visitors, guests) who have access to and are users of school digital systems, both in and out of the school. It also applies to the use of personal digital technology on the school site (where allowed).

Table of Contents

Development/monitoring/review of this policy

This Online Safety policy has been developed by the Online Safety Working Group made up of:

- Headteacher/senior leaders
- Online safety officer/coordinator
- Staff – including practitioners/support staff/technical staff
- Governors
- Parents

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 *Chair & Vice Chair of Governors*	*15th April 2021*
The implementation of this online safety policy will be monitored by the:	*Online Safety Working Group – Chaired by Lee Small – Assistant Head*
Monitoring will take place at regular intervals:	*Annually – Prior to Sept*
The *governing body/governors sub-committee* will receive a report on the implementation of the online safety policy generated by the monitoring group (which will include anonymous details of online safety incidents) at regular intervals:	*In line with the school policy review process*
The online safety policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to online safety or incidents that have taken place. The next anticipated review date will be:	*Annually – July (Prior to school Governing body meeting)*
Should serious online safety incidents take place, the following external persons/agencies should be informed:	*Relevant parties stated in the school Safeguarding Policy*

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:
    - ➢ pupils
    - ➢ parents and 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 online safety 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 should take on the role of online safety governor to include:

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

Headteacher and senior leaders

- The headteacher has a duty of care for ensuring the safety (including online safety) of members of the school community, though the day to day responsibility for online safety may be delegated to the online safety coordinator/officer.
- The headteacher and (at least) another member of the senior leadership team should be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff.
- The headteacher/senior leaders are responsible for ensuring that the online safety coordinator/officer and other relevant staff receive suitable training to enable them to carry out their online safety roles and to train other colleagues, as relevant.
- The headteacher/senior leaders will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal online safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.
- The headteacher/senior leaders will receive regular monitoring reports from the online safety coordinator/officer.

Online safety coordinator/officer

The online safety coordinator/officer:

- leads the online safety group
- takes day to day responsibility for online safety issues and has a leading role in establishing and reviewing the school online safety policies/documents
- ensures that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place
- provides (or identifies sources of) training and advice for staff
- liaises with the local authority/relevant body
- liaises with (school/local authority) technical staff
- receives reports of online safety incidents and creates a log of incidents to inform future online safety developments
- meets regularly with online safety governor to discuss current issues, review incident logs and if possible, filtering change control logs
- attends relevant meeting/sub-committee of governors
- reports regularly to headteacher/senior leadership team.

Network manager/technical staff

The network manager/technical staff is responsible for ensuring that:

- the school technical infrastructure is secure and is not open to misuse or malicious attack
- the school meets (as a minimum) the required online safety technical requirements as identified by the local authority or other relevant body and also the online safety policy/guidance that may apply
- users may only access the networks and devices through a properly enforced password protection policy.
- they keep up-to-date with online safety technical information in order to effectively carry out their online safety role and to inform and update others as relevant

- the use of the network/internet/learning platform/remote access/e-mail is regularly monitored in order that any misuse/attempted misuse can be reported to the senior leader, online safety coordinator/officer, DSP for investigation/action/sanction
- monitoring software/systems are implemented and updated regularly
- web filtering is applied and updated on a regular basis and its implementation is not the sole responsibility of any single person.

Teaching and support staff

These individuals are responsible for ensuring that:

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

Designated senior person

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

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

Online safety group

The online safety group provides a consultative group that has wide representation from the school community, with responsibility for issues regarding online safety and monitoring the online safety policy including the impact of initiatives. The group will also be responsible for regular reporting to senior leaders and the governing body.

Members of the online safety group (or other relevant group) will assist the online safety coordinator/officer 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 education provision – ensuring relevance, breadth and progression
- monitoring network/internet/incident logs where possible
- consulting stakeholders – including parents/carers and pupils about the online safety provision
- monitoring improvement actions identified through use of the 360 degree safe tool.

Pupils

These individuals:

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

Parents and carers

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

- digital and video images taken at school events
- access to parents'/carers' sections of the website, school app and online pupil records
- their children's personal devices in school.

Policy statements

Education – pupils

While regulation and technical solutions are very important, their use must be balanced by educating pupils to take a responsible approach. The education of pupils in online safety is therefore an essential part of the school's online safety provision. Pupils 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. Computing/PSHE) and topic areas and should be regularly revisited
- key online safety messages should be reinforced as part of a planned programme of assemblies and tutorial/pastoral activities
- pupils should be taught in all lessons to be critically aware of the materials/content they access online and be guided to validate the accuracy of information
- pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- pupils should be supported in building resilience to radicalisation by providing a safe environment for debating controversial issues and helping them to understand how they can influence and participate in decision-making.
- pupils 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.
- where pupils are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites pupils visit
- it is accepted that from time to time, for good educational reasons, pupils may need to research topics, (e.g. racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the technical staff (or other nominated person) can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need.

Education – parents and carers

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

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

- letters, newsletters, web site, school app
- parents and carers evenings/sessions
- high profile events/campaigns, e.g. Safer Internet Day, Device Rollout Evenings
- reference to the relevant web sites/publications, e.g. www.saferinternet.org.uk/ 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
- the school website will provide online safety information for the wider community, as required
- supporting community groups, e.g. early years settings, childminders, youth/sports/voluntary groups to enhance their online safety provision.

Education and training – staff/volunteers

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

- a planned programme of formal online safety training will be made available to staff. This will be regularly updated and reinforced. An audit of the online safety training needs of all staff will be carried out regularly
- 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/officer (or other nominated person) will receive regular updates through attendance at external training events, (e.g. from Consortium/ LA/other relevant organisations) and by reviewing guidance documents released by relevant organisations
- this online safety policy and its updates will be presented to and discussed by staff in staff/team meetings/INSET days
- the online safety coordinator/officer (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 such as:

- attendance at training provided by the local authority/National Governors Association/or other relevant organisation
- 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 need to ensure that the relevant people named in the above sections will be effective in carrying out their online safety responsibilities:

- school technical systems will be managed in ways that ensure that the school meets recommended technical requirements
- there will be regular reviews and audits of the safety and security of school technical systems
- servers, wireless systems and cabling must be securely located and physical access restricted
- good practice in preventing loss of data from ransomware attacks requires a rigorous and verified back-up routine, including the keeping of copies in multiple locations
- all school networks and systems will be protected by secure passwords
- the master account passwords for the school systems should be kept in a secure place, e.g. school safe. consideration should also be given to using two factor authentication for such accounts
- all users have clearly defined access rights to school technical systems and devices. Details of the access rights available to groups of users will be recorded by the Network Manager (or other person) and will be reviewed, at least annually
- all users (adults and pupils) have responsibility for the security of their username and password, must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security
- passwords must not be shared with anyone

- all users will be provided with a username and password by the ICT Support who will keep an up to date record of users and their usernames
- passwords should be long and sufficiently secure, in-line with recommended practice
- the Network Manager is responsible for ensuring that software licence logs are accurate and up-to-date and that regular checks are made to reconcile the number of licences purchased against the number of software installations
- internet access is filtered for all users. Illegal content (child sexual abuse images) is filtered by the internet and filtering/firewall 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/hierarchy in place to deal with requests for filtering changes
- the school has provided enhanced/differentiated user-level filtering, allowing different filtering levels for different groups of users
- internet filtering should ensure that children are safe from terrorist and extremist material when accessing the internet
- where possible, school technical staff regularly monitor and record the activity of users on the school technical systems and users are made aware of this in the acceptable use agreement
- an appropriate system is in place for users to report any actual/potential technical incident/security breach to the relevant person
- appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, workstations, mobile devices, etc., from accidental or malicious attempts which might threaten the security of the school systems and data. These are tested regularly. The school infrastructure and individual devices are protected by up to date virus software
- an agreed policy is in place for the provision of temporary access of 'guests', (e.g. supply teachers, visitors) onto the school systems
- an agreement is in place regarding the extent of personal use that users (staff/pupils/guests/visitors) and their family members are allowed on school devices that may be used out of school
- an agreed policy is in place that allows staff to/forbids staff from downloading executable files and installing programmes on school devices.

An agreed policy is in place regarding the use of removable media (e.g. memory sticks/CDs/DVDs) by users on school devices. Personal data should not be sent over the internet or taken off the school site unless safely encrypted or otherwise secured. Systems are in place to facilitate such communications, as required.

Mobile technologies

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

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

In preparing a mobile technologies policy the school considers possible issues and risks, which include:

- security risks in allowing connections to the school network
- filtering of personal devices
- breakages and insurance
- access to devices for all pupils
- avoiding potential classroom distraction
- network connection speeds, types of devices
- charging facilities
- total cost of ownership.

In addition to the points above.

- The school Acceptable Use Agreements for staff, pupils, parents and carers will give consideration to the use of mobile technologies.

	School devices			Personal devices	
	School owned for individual use	School owned for multiple users	Authorised device[1]	Pupil owned	Staff owned
Allowed in school	Yes	Yes	Yes	No	Limited[3]
Full network access	Yes	Yes	Limited	No	No
Internet only	N/A	N/A	N/A	No	Yes[4]

Aspects that the school currently considers and includes in our Online Safety policy and Acceptable Use Agreements include the following:

School owned/provided devices:

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

Personal / Authorised devices

- Which users are allowed to use personal mobile devices in school (staff/pupils/visitors).
- Restrictions on where, when and how they may be used in school.
- Storage.
- Whether staff will be allowed to use personal devices for school business.
- Levels of access to networks/internet (as above).
- Network/broadband capacity.
- Technical support.
- Filtering of the internet connection to these devices.
- Data protection.
- Taking/storage/use of images.
- Liability for loss/damage or malfunction following access to the network (likely to be a disclaimer about school responsibility).
- Identification/labelling of personal devices.

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

[3&4] Staff personal device are permitted in school for emergency use only and have restricted internet only access where requested for school use

- How visitors will be informed about school requirements.
- How education about the safe and responsible use of mobile devices is included in the school online safety education programmes.

Use of digital and video images

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

- When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet, e.g. on social networking sites.
- 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 or videos should not include other children, be published/made publicly available on social networking sites, nor should parents/carers comment on any activities involving other pupils 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; the personal equipment of staff should not be used for such purposes.
- Care should be taken when taking digital/video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Pupils must not take, use, share, publish or distribute images of others without their permission.
- Photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with good practice guidance on the use of such images.
- Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs.
- Written consent from parents or carers will be obtained before photographs of pupils are published on the school website.
- Pupils' work can only be published with the consent 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
- 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 is developing and implementing a "retention schedule" to support this
- data held must be accurate and up to date where this is necessary for the purpose it is held and 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 looks after their data and what their rights are in a clear Privacy Notice (see Privacy Notice section in the appendix)
- procedures must be in place to deal with the individual rights of the data subject, e.g. one of the dozen rights applicable is that of Subject Access which enables an individual to see to have a copy of the personal data held about them
- Data Protection Impact Assessments (DPIA) are carried out where necessary. For example, to ensure protection of personal data when accessed using any remote access solutions, or entering into a relationship with a new supplier
- IT system security is ensured and regularly checked. Patches and other security essential updates are applied promptly to protect the personal data on the systems
- 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
- 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” or “locked” at the end of any session in which they are using personal data
- transfer data using encryption and secure password protected devices.

Communication technologies

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

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

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

- the official school e-mail service may be regarded as safe and secure and is monitored. Users should be aware that e-mail communications are monitored. Staff and pupils should therefore use only the school email service to communicate with others when in school, or on school systems
- users must immediately report to a member of the ICT Support Team or relevant member of staff (e.g. Pastoral Co-ordinator) – 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 pupils 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
- pupils are taught about online safety issues, such as the risks attached to the sharing of personal details. They are 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 any internet platform and only official e-mail addresses should be used to identify members of staff.

Social media

Expectations for teachers' professional conduct are set out by the Department for Education (DfE,) 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 pupils and staff. Schools and local authorities could be held responsible, indirectly for acts of their employees in the course of their employment. Staff members who harass, bully online, discriminate on the grounds of sex, race or disability or who defame a third party may render the school or local authority liable to the injured party. Reasonable steps to prevent predictable harm must be in place. All staff working at any educational establishment are expected to demonstrate a professional approach and respect for pupils 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 pupils 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 pupils, 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 personal social media accounts. In all cases, where a personal account is used which associates itself with, or impacts on, the school it must be made clear that the member of staff is not communicating on behalf of the school with an appropriate disclaimer. Such personal communications are within the scope of this policy.
- Personal communications which do not refer to or impact upon the school are outside the scope of this policy.
- Where excessive personal use of social media in school is suspected, and considered to be interfering with relevant duties, disciplinary action may be taken.
- The school permits reasonable and appropriate access to private social media sites.

Monitoring of public social media

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

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

Unsuitable/inappropriate activities

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

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

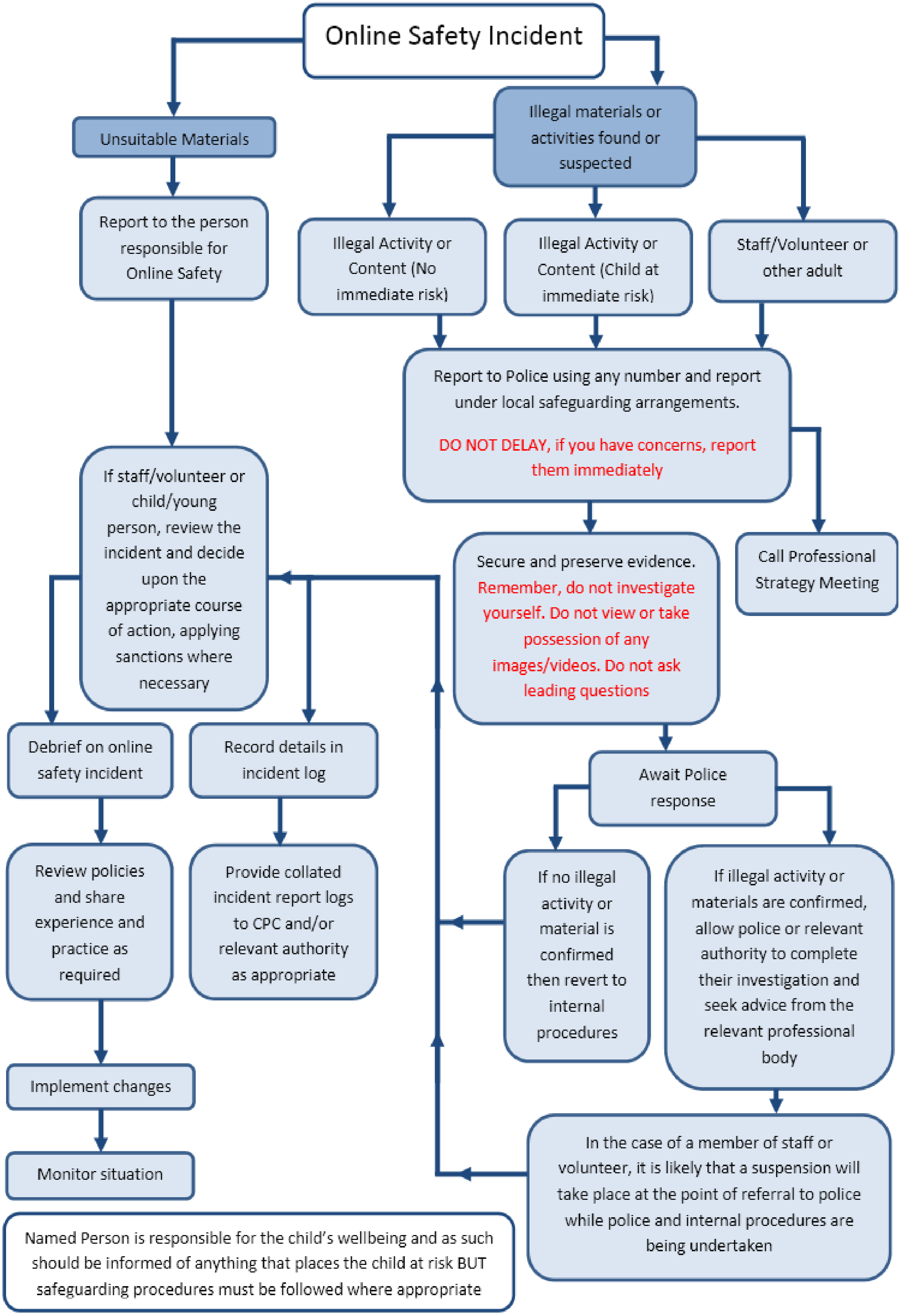
User actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Users shall not visit internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	child sexual abuse images – the making, production or distribution of indecent images of children, contrary to The Protection of Children Act 1978					X
	grooming, incitement, arrangement or facilitation of sexual acts against children Contrary to the Sexual Offences Act 2003					X
	possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character), contrary to the Criminal Justice and Immigration Act 2008					X
	criminally racist material in UK – to stir up religious hatred (or hatred on the grounds of sexual orientation) - contrary to the Public Order Act 1986					X
	pornography				X	
	promotion of any kind of discrimination				X	
	threatening behaviour, including promotion of physical violence or mental harm				X	
	promotion of extremism or terrorism				X	
	any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute				X	
Using school systems to run a private business					X	
Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school					X	
Infringing copyright					X	
Revealing or publicising confidential or proprietary information, (e.g. financial/personal information, databases, computer/network access codes and passwords)					X	
Creating or propagating computer viruses or other harmful files					X	
Unfair usage (downloading/uploading large files that hinders others in their use of the internet)					X	
Online gaming (educational)			X			
Online gaming (non educational)			X			
Online gambling					X	
Online shopping/commerce			X			
File sharing			X			
Use of social media			X	X		
Use of messaging apps			X	X		
Use of video broadcasting, e.g. YouTube			X	X		

Responding to incidents of misuse

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

Illegal incidents

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



Online Safety Incident

Unsuitable Materials

Report to the person responsible for Online Safety

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

Debrief on online safety incident

Review policies and share experience and practice as required

Implement changes

Monitor situation

Record details in incident log

Provide collated incident report logs to CPC and/or relevant authority as appropriate

Illegal materials or activities found or suspected

Illegal Activity or Content (No immediate risk)

Illegal Activity or Content (Child at immediate risk)

Staff/Volunteer or other adult

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

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

Call Professional Strategy Meeting

Secure and preserve evidence. Remember, do not investigate yourself. Do not view or take possession of any images/videos. Do not ask leading questions

Await Police response

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

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

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

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

Other incidents

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

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

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

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

School actions

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

Pupil actions

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

Staff Actions

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

Appendices – Section A - Acceptable Use Agreement

- A2 Pupil Acceptable Use agreement template (older children)
- A3 Staff and Volunteers Acceptable Use Agreement template
- A4 Parents /Carers Acceptable Use Agreement template
- A5 Guests / visitors Acceptable Use Agreement template

Appendices – Section B – Specific Policies

- B1 Technical security policy
- B2 Mobile technologies policy
- B3 Social media policy template
- B4 Online safety group terms of reference

Appendices – Section C – Supporting documents and links

- C1 Responding to incidents of misuse – flowchart

A2 Pupil Acceptable Use Agreement (AUA)

School policy

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

This Acceptable use agreement is intended to ensure:

- that pupils 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 pupils will have good access to digital technologies to enhance their learning and will, in return, expect the pupils to agree to be responsible users.

Acceptable use agreement

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

For my own personal safety:

- I understand that the school will monitor my use of 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 will not write down or store a password where it is possible that someone may steal it
- I will be aware of "stranger danger", when I am communicating online
- I will not disclose or share personal information about myself or others when online (this could include names, addresses, email addresses, telephone numbers, age, gender, educational details, financial details, etc.)
- I will not arrange to meet people off-line that I have communicated with online
- I will immediately report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it online.

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

- I understand that the school systems and devices are primarily intended for educational use and that I will only use them for personal or recreational use if I have permission
- I will only make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work, if I have permission
- I will only use the school systems or devices for online gaming, internet shopping/e-commerce, file sharing, or video broadcasting (e.g. YouTube), if I have permission of a member of staff to do so.

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

- I will respect others' work and property and will only access, copy, remove or alter any other user's files, with the owner's knowledge and permission
- I will be polite and responsible when I communicate with others, I will not use strong, aggressive or inappropriate language and I appreciate that others may have different opinions
- I will only take or distribute images of others with their permission.

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

- I will only use my device(s) in school if I have permission. I understand that, if I do use my device(s) in the school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment

- I understand the risks and will not try to upload, download or access any materials which are illegal or inappropriate or may cause harm or distress to others, nor will I try to use any programmes or software that might allow me to bypass the filtering/security systems in place to prevent access to such materials
- I will immediately report any damage or faults involving equipment or software, however this may have happened
- I will only open hyperlinks in emails or attachments to emails, if I know and trust the person/organisation who sent the email, and have no concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes)
- I will only install/ store programmes on a device, if I have permission and this software will not impact on the ability to use the device for learning
- 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 online bullying, use of images or personal information)
- I understand that if I fail to comply with this acceptable use agreement, I will be subject to disciplinary action. This may include loss of access to the school network/internet, detentions, other sanctions and contact with parents and in the event of illegal activities involvement of the police.

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

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 systems.

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

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

Name of Pupil: --

Form Group --

Signed: --

Date: --

A3 Staff (and volunteer) Acceptable Use Agreement

School policy

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

This Acceptable Use Agreement is intended to ensure:

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

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

Acceptable Use Agreement

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

For my professional and personal safety:

- I understand that the school will monitor my use of the ICT systems, email and other digital communications
- I understand that the rules set out in this agreement also apply to use of school ICT systems (e.g. laptops, email, online platforms etc.) out of school, and to the transfer of personal data (digital or paper based) out of school
- I understand that the school digital technology systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within the policies and rules set down by the school
- I will not disclose my 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 anywhere
- I will immediately report any illegal, inappropriate or harmful material or incident I become aware of to the appropriate person.

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

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

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

- When I use my mobile devices/ laptops/mobile phones/USB devices etc.) in school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment. I will also follow any additional rules set by the school about such use. I will ensure that any such devices are protected by up to date anti-virus software and are free from viruses
- I will not use personal email addresses on the school digital technology systems
- I will not open any hyperlinks in emails or any attachments to emails, unless the source is known and trusted, or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes)
- I will ensure that my data is regularly backed up, in accordance with relevant school policies
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, extremist material or adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering/security systems in place to prevent access to such materials
- I will only make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work, with permission
- I will only install or attempt to install/store programmes on devices after seeking advice
- 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 Data Protection 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 digital technology equipment in school, but also applies to my use of school systems and equipment off the premises and my use of personal equipment on the premises or in situations related to my employment by the school
- I understand that if I fail to comply with this acceptable use agreement, I could be subject to disciplinary action. This could include a warning, a suspension, referral to Governors and/or the Local Authority and in the event of illegal activities the involvement of the police.

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

Staff/Volunteer Name: --

Signed: --

Date: --

A4 Parent/Carer Acceptable Use Agreement

Digital technologies have become integral to the lives of children and young people, both within school and outside school. These technologies provide powerful tools, which create 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 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
- school systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk
- parents and carers are aware of the importance of online safety and are involved in the education and guidance of young people with regard to their online behaviour.

The school will try to ensure that pupils will have good access to digital technologies to enhance their learning and will, in return, expect pupils 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's 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:... Pupil's Name ....

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

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.

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

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

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

Signed .... Date: ....

A4.1 Use of Digital/Video Images

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

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

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

In accordance with guidance from the Information Commissioner's Office, parents/carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use 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 pupils in the digital / video images.

Please refer to the school's latest Data Protection Policy for more information.

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

A4.2 Digital/Video Images Permission Form

Parent/Carers Name: ---

Pupil Name(s): ---

As the parent /carer of the above pupil, I agree to the school taking digital/video images of my child/children.	Yes / No
I agree to these images being used: • to support learning activities.	Yes / No
• in publicity that reasonably celebrates success and promotes the work of the school. This will include examples such as school websites, social media platforms, other publications/presentations celebrating the success of the school/pupils	Yes / No
I agree that if I take digital or video images at, or of – school events which include images of children other than my own, I will abide by these guidelines in my use of these images.	Yes / No

Signed: ---

A4.3 Use of Biometric Systems

The school uses biometric systems for the recognition of individual pupils for use in the Cashless Catering system

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

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

Please refer to the school's latest Data Protection Policy for more information.

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

Parent/Carer Name: --

Pupil Name(s): ---

As the parent /carer of the above pupil(s), I agree to the school using biometric recognition systems, as described above	Yes / No
I understand that the images cannot be used to create a whole fingerprint of my child and that these images will not be shared with anyone outside the school	Yes / No

Signed: --

A4.4 Use of Cloud Systems Permission Form

The school uses a variety of digital platforms, for example Microsoft 365, Doddle, ClassCharts, GCSEPod, LBQ, and Sparx, for pupils and staff. This permission form describes the tools and pupil responsibilities for using these services.

The above services are available to each pupil as part of the school's online presence in the above provides.

Using these services will enable your child to collaboratively create, edit and share files and websites for school related projects and communicate via email with other pupils and members of staff. These services are entirely online and available 24/7 from any internet-connected computer.

The school believes that use of the tools significantly adds to your child's educational experience.

Please refer to the school's latest Data Protection Policy for more information.

Do you consent to your child to having access to this service?	Yes / No

Pupil Name(s): --

Parent / Carers Name: --

Signed: --

Date: --

A5 Acceptable Use Agreement for guests / visitors

This Acceptable Use Agreement is intended to ensure:

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

Acceptable Use agreement

I understand that I must use school systems and devices in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems, devices and other users. This agreement will also apply to any personal devices that I bring into the school.

- I understand that my use of school systems and devices and digital communications will be monitored.
- I will not use a personal device that I have brought into school for any activity that would be inappropriate in a school setting.
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, extremist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering/security systems in place to prevent access to such materials.
- I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person.
- I will not access, copy, remove or otherwise alter any other user's files, without permission.
- I will ensure that if I take and/or publish images of others I will only do so with their permission and in line with school policies. I will not use my personal equipment to record these images, without permission. If images are published it will not be possible to identify by name, or other personal information, those who are featured.
- I will not publish or share any information I have obtained whilst in the school on any personal website, social networking site or through any other means, unless I have permission from the school.
- I will not, without permission, make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not install or attempt to install programmes of any type on a school device, nor will I try to alter computer settings, unless I have permission to do so.
- I will not disable or cause any damage to school equipment, or the equipment belonging to others.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.
- I will ensure that I have permission to use the original work of others in my own work.
- Where work is protected by copyright, I will not download or distribute copies (including music and videos).
- I understand that if I fail to comply with this Acceptable Use Agreement, the school has the right to remove my access to school systems/devices.

Please refer to the school's latest Data Protection Policy for more information.

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

Name ………………………………… Signed ………………………………… Date: ……………

B1 School technical security policy template (including filtering and passwords)

Introduction

Effective technical security depends not only on technical measures, but also on appropriate policies and procedures and on good user education and training. The school will be responsible for ensuring that the school infrastructure/network is as safe and secure as is reasonably possible and that:

- users can only access data to which they have right of access
- no user should be able to access another's files (other than that allowed for monitoring purposes within the school's policies)
- access to personal data is securely controlled in line with the school's personal data policy
- logs are maintained of access by users and of their actions while users of the system
- there is effective guidance and training for users
- there are regular reviews and audits of the safety and security of school computer systems
- there is oversight from senior leaders and these have impact on policy and practice.

Responsibilities

The management of technical security will be the responsibility of The Network Manager.

Technical Security

Policy statements

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

- 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
- appropriate security measures are in place to protect the servers, firewalls, switches, routers, wireless systems, work stations, mobile devices etc. from accidental or malicious attempts which might threaten the security of the school systems and data
- responsibilities for the management of technical security are clearly assigned to appropriate and well trained staff
- all users will have clearly defined access rights to school technical systems defined by their role as a member of staff or as a pupil
- users will be made responsible for the security of their username and password, must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security
- The Network Manager is responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations
- mobile device security and management procedures are in place
- 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
- remote management tools are used by staff to control workstations and view users activity
- an appropriate system is in place for users to report any actual/potential technical incident to the online safety co-ordinator/network manager/technician
- an agreed policy is in place for the provision of temporary access of guests / visitors, (e.g. trainee teachers, supply teachers, visitors) onto the school system
- an agreed policy is in place within respective policies regarding the downloading of executable files and the installation of programmes on school devices by users

- an agreed policy is in place within respective policies regarding the extent of personal use that users (staff/pupils/guests/visitors) and their family members are allowed on school devices that may be used out of school
- an agreed policy is in place in line with the schools GDPR policy regarding the use of removable media (e.g. memory sticks/CDs/DVDs) by users on school devices
- the school infrastructure and individual workstations are protected by up to date software to protect against malicious threats from viruses, worms, trojans etc.
- personal data should not be sent over the internet or taken off the school site unless safely encrypted or otherwise secured.

Password Security

A safe and secure username/password system is essential if the above is to be established and will apply to all school technical systems, including networks, devices, email and learning platform.

Policy Statements:

- These statements apply to all users.
- All school networks and systems will be protected by secure passwords.
- All users have clearly defined access rights to school technical systems and devices. Details of the access rights available to groups of users will be recorded by the Network Manager (or other person) and will be reviewed, at least annually, by the online safety group (or other group).
- All users (adults and pupils) have responsibility for the security of their username and password, must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security.
- Passwords must not be shared with anyone.
- All users will be provided with a username and password by the ICT Team who will keep an up to date record of users and their usernames.

Password requirements:

- Staff Passwords should be a minimum 8 Characters with a mixture of upper and lower case, including at least one number or special character. Good practice highlights:
  - passwords over 12 characters in length are considerably more difficult to compromise than shorter passwords
  - passwords generated by using a combination of unconnected words that are over 16 characters long are extremely difficult to crack
  - password length trumps any other special requirements such as uppercase/lowercase letters, number and special characters
  - passwords should be easy to remember, but difficult to guess or crack
  - passwords should be different for different accounts, to ensure that other systems are not put at risk if one is compromised and should be different for systems used inside and outside of school
  - passwords must not include names or any other personal information about the user that might be known by others
- Passwords must be changed on first login to the system.

Pupil passwords:

- Records of pupil usernames and passwords are securely kept when not required by the user.
- Passwords will be required to change if it is thought to be compromised.
- Pupils will be taught the importance of password security, this should include how passwords are compromised, and why these password rules are important.

Notes for technical staff/teams

- Each administrator should have an individual administrator account, as well as their own user account with access levels set at an appropriate level. Consideration is also be given to using two factor authentication for such accounts.
- There are multiple redundancies to gain domain admin level access to the network, should this be required.

- It is good practice that where passwords are used there is a user-controlled password reset process to enable independent, but secure re-entry to the system. This ensures that only the owner has knowledge of the password.
- Where user-controlled reset is not possible, passwords for new users, and replacement passwords for existing users will be allocated by the ICT Team
- This password is temporary and the user is forced to change their password on first login. The generated passwords should also be long and random.
- Requests for password changes should be authenticated by ICT Team to ensure that the new password can only be passed to the genuine use.
- Suitable arrangements are in place to provide guests/visitors/supply with appropriate access to systems which expires after use.
- In good practice, the account is "locked out" for an amount of time following six successive incorrect log-on attempts.

Training/Awareness:

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

- at induction
- through the school's online safety policy and password security policy
- through the acceptable use agreement.

Pupils will be made aware of the school's password policy:

- in Computing lessons by teachers
- through the Acceptable Use Agreement.

Audit/Monitoring/Reporting/Review:

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

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

Filtering

Introduction

The filtering of internet content provides an important means of preventing users from accessing material that is illegal or is inappropriate in an educational context. The filtering system cannot, however, provide a 100% guarantee that it will do so, because the content on the web changes dynamically and new technologies are constantly being developed. It is important, therefore, to understand that filtering is only one element in a larger strategy for online safety and acceptable use. It is important that the school has a filtering policy to manage the associated risks and to provide preventative measures which are relevant to the situation in this school.

Responsibilities:

The responsibility for the management of the school filtering policy will be held by the IT Network Manager. They will manage the school filtering, in line with this policy and will keep records/logs of changes and of breaches of the filtering systems.

To ensure that there is a system of checks and balances and to protect those responsible, changes to the school filtering service must

- be logged in change control logs within the filtering system
- be reported to a second responsible person, the IT Department Line Manager.

All users have a responsibility to report immediately to the ICT Team any infringements of the school's filtering policy of which they become aware or any sites that are accessed, which they believe should have been filtered.

Users must not attempt to use any programmes or software that might allow them to bypass the filtering/security systems in place to prevent access to such materials.

Policy Statements:

Internet access is filtered for all users. Differentiated internet access is available for staff and customised filtering changes are managed by the school. Illegal content is filtered by broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list and other illegal content lists. Filter content lists are regularly updated and internet use is logged and frequently monitored. Ideally, the monitoring process alerts the school to breaches of the filtering policy, which are then acted upon. There is a clear route for reporting and managing changes to the filtering system. Where personal mobile devices are allowed internet access through the school network, filtering will be applied that is consistent with school practice.

- The school manages its own filtering service.
- The school has provided enhanced/differentiated user-level filtering through the use of the Sophos filtering programme allowing different filtering levels for different groups of users – staff/pupils/guest, etc.
- In the event of the technical staff needing to switch off the filtering for any reason, or for any user, this must be logged and carried out by a process that is agreed by the IT Department Line Manager.
- Mobile devices that access the school internet connection (whether school or personal devices) will be subject to the same filtering standards as other devices on the school systems.
- Any filtering issues should be reported immediately to the filtering provider.
- Requests from staff for sites to be removed from the filtered list will be considered by the technical staff or Service Provider. If the request is agreed, this action will be recorded and logs of such actions shall be reviewed regularly by the online safety group.

Education/Training/Awareness:

Pupils will be made aware of the importance of filtering systems through the online safety education programme. They will also be warned of the consequences of attempting to subvert the filtering system.

Staff users will be made aware of the filtering systems through:

- the Acceptable Use Agreement
- induction training
- staff meetings, briefings, training sessions

Parents/ carers will be informed of the school's filtering policy through the Acceptable Use Agreement and through online safety awareness sessions etc.

Changes to the Filtering System:

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

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

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

Monitoring:

No filtering system can guarantee 100% protection against access to unsuitable sites. The school will therefore monitor the activities of users on the school network and on school equipment as indicated in the school online safety policy and the Acceptable Use Agreements. Monitoring will take place using Impero Safeguarding Software on all school devices utilising predefined government derived watch words.

Audit/Reporting:

Logs of filtering change controls and of filtering incidents will be made available to; the Pastoral Teams and SLT

- ICT team
- Pastoral and Safeguarding teams
- online safety governor/governors committee
- external filtering provider/local authority/police on request

The filtering policy will be reviewed in the response to the evidence provided by the audit logs of the suitability of the current provision.

Further Guidance:

- NEN Technical guidance: http://www.nen.gov.uk/e-security-managing-and-maintaining-e-securitycyber-security-in-schools/
- NEN –School e-Security Checklist
- Somerset Technical Guidance for schools – this checklist is particularly useful where a school uses external providers for its technical support/security:
- Prevent duty - schools in England (and Wales) are required *"to ensure children are safe from terrorist and extremist material when accessing the internet in school, including by establishing appropriate levels of filtering"* (Revised Prevent Duty Guidance: for England and Wales, 2015).
- 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.
- In response to the above, the UK Safer Internet Centre produced guidance for schools on "Appropriate filtering and appropriate monitoring".

B2 - School Mobile Technologies Policy (inc. BYOD/BYOT)

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

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

Potential benefits of mobile technologies

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

Considerations

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

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

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

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

	School Devices			Personal Devices		
	School owned and allocated to a single user	School owned for use by multiple users	Authorised / 121 device[2]	Pupil owned	Staff owned	Visitor / Guest owned
Allowed in school	Yes	Yes	Yes	Yes	Yes	Yes
Full network access	*Yes*	*Yes*	*Yes*	No	No	No
Internet only				No	Yes	Yes
No network access						

School devices

- All school/one-to-one devices are controlled though the use of mobile device management (MDM) software.
- Appropriate access control is applied to all mobile devices according to the requirements of the user (e.g. internet only access, network access allowed, shared folder network access).
- All school/one-to-one devices must be suitably protected via a passcode/password/pin (and encryption where relevant). Those devices allocated to members of staff must only be accessed and used by members of staff.
- Appropriate exit processes are implemented for devices no longer used at a school location or by an authorised user. These may include; revoking the link between MDM software and the device, ensuring no sensitive data is removed from the network and uninstalling school-licenced software etc.
- The software/apps originally installed by the school must remain on the school owned device in usable condition and be easily accessible at all times. From time to time the school may add software applications for use in lesson. Periodic checks of devices will be made to ensure that users have not removed required apps.
- The school will ensure that school devices contain the necessary apps for school work. Apps added by the school will remain their property and will not be accessible to pupils on authorised devices once they leave the school roll. Any apps bought by the user on their own account will remain theirs.
- The school is responsible for keeping devices up to date through software, security and app updates. The device is virus protected and should not be capable of passing on infections to the network. Where user intervention or support for this process is required, this will be made clear to the user.
- School devices are provided to support learning. It is expected that pupils will bring devices to school as part of their normal equipment.
- The changing of settings (exceptions include personal settings such as font size, brightness, etc.) that would stop the device working as it was originally set up and intended is not permitted.
- All school devices are subject to routine monitoring.
- Pro-active monitoring has been implemented to monitor activity.

Personal devices

Where personal device are permitted to be used in line with the school's Behaviour Policy, the following guidance must be followed and users need to be aware of the risks and restrictions of use.

- All personal devices are restricted through the implementation of technical solutions that provide appropriate levels of filtered network access.

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

- Personal devices are brought into the school entirely at the risk of the owner and the decision to bring the device in to the school lies with the user (and their parents/carers) as does the liability for any loss or damage resulting from the use of the device in the school.
- Staff personal devices should not be used to contact pupils or their families, nor should they be used to take images of pupils.
- The school accepts no responsibility or liability in respect of lost, stolen or damaged devices while at the school or on activities organised or undertaken by the school (the school recommends insurance is purchased to cover that device whilst out of the home).
- The school accepts no responsibility for any malfunction of a device due to changes made to the device while on the school network or whilst resolving any connectivity issues.
- The school recommends that the devices are made easily identifiable and have a protective case to help secure them as the devices are moved around the school. Passcodes or PINs should be set on personal devices to aid security.
- The school is not responsible for the day to day maintenance or upkeep of the user's personal device such as the charging of any device, the installation of software updates or the resolution of hardware issues.
- Personal devices should be charged before being brought to the school as the charging of personal devices is not permitted during the school day.

User behaviour

Users are expected to act responsibly, safely and respectfully in line with current Acceptable Use Agreements, in addition:

- the sending of abusive or inappropriate messages or content via mobile phones or personal devices is forbidden by any member of the community and any breaches will be dealt with as part of the Behaviour policy
- guidance is made available by the school to users concerning where and when mobile devices may be used
- devices may not be used in tests or exams
- users are responsible for keeping their device up to date through software, security and app updates. The device is virus protected and should not be capable of passing on infections to the network
- users are responsible for charging their own devices and for protecting and looking after their devices while in the school
- personal devices must be at least in silent mode or switched off on the school site
- users should be mindful of the age limits for app purchases and use and should ensure they read the terms and conditions before use
- pupils must not photograph or video people using personal devices
- devices may be used in lessons in accordance with teacher direction
- staff owned devices should not be used for personal purposes during teaching sessions, except in emergency situations
- printing from personal devices will not be possible.

Visitors / Guests

Visitors will be provided with information about how, where and when they are permitted to use mobile technology on the site, in line with local safeguarding arrangements. They will also be informed about the school policy on taking images.

Insurance

In line with the schools implemented one-to-one provision (authorised devices/1:1) the school has arranged insurance for these devices.

The claims process for any one-to-one / authorised device is dealt with by the ICT Team directly with the insurance provider. The device is swapped out temporarily whilst the claim/repair/replacement is made and then returned when complete. All devices are provided a 3-year Accidental Damage and Theft cover which runs from the day they are handed out to pupils.

B3 Social Media Policy

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

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

Scope

This policy is subject to the school's Behaviour policy and Acceptable Use Agreements.

This policy:

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

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

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

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

Personal communications which do not refer to or impact upon the school are outside the scope of this policy.

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

Organisational control

Roles & Responsibilities

- Senior Leadership Team (SLT)
  - facilitating training and guidance on Social Media use
  - developing and implementing the Social Media policy
  - taking a lead role in investigating any reported incidents
  - making an initial assessment when an incident is reported and involving appropriate staff and external agencies as required
  - receive completed applications for Social Media accounts
  - approve account creation

- Administrator / Moderator
  - create the account following SLT approval
  - store account details, including passwords securely
  - be involved in monitoring and contributing to the account
  - control the process for managing an account after the lead staff member has left the school (closing or transferring)

- Staff
  - know the contents of and ensure that any use of social media is carried out in line with this and other relevant policies
  - attending appropriate training
  - regularly monitoring, updating and managing content he/she has posted via school accounts
  - adding an appropriate disclaimer to personal accounts when naming the school

Managing accounts

- Process for creating new accounts
  The school community is encouraged to consider if a social media account will help them in their work, e.g. a history department Twitter account, or a "Friends of the school" Facebook page. Anyone wishing to create such an account must present a business case to the school Senior Leadership Team which covers the following points:-
  - the aim of the account
  - the intended audience
  - how the account will be promoted
  - who will run the account (at least two staff members should be named)
  - will the account be open or private/closed

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

Monitoring

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

Behaviour

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

Legal considerations

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

Handling abuse

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

Tone

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

Use of images

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

Personal use

Staff

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

Pupils

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

Parents/Carers

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

Monitoring posts about the school

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

Appendix

Managing your personal use of Social Media:

- “nothing” on social media is truly private
- social media can blur the lines between your professional and private life. Don’t use the school logo and/or branding on personal accounts
- check your settings regularly and test your privacy
- keep an eye on your digital footprint
- keep your personal information private
- regularly review your connections – keep them to those you want to be connected to
- when posting online consider; Scale, Audience and Permanency of what you post
- if you want to criticise, do it politely
- take control of your images – do you want to be tagged in an image? What would children or parents say about you if they could see your images?
- know how to report a problem.

Managing school social media accounts

The Do’s

- Check with a senior leader before publishing content that may have controversial implications for the school.
- Use a disclaimer when expressing personal views.
- Make it clear who is posting content.
- Use an appropriate and professional tone.
- Be respectful to all parties.
- Ensure you have permission to ‘share’ other peoples’ materials and acknowledge the author.
- Express opinions but do so in a balanced and measured manner.
- Think before responding to comments and, when in doubt, get a second opinion.
- Seek advice and report any mistakes using the school’s reporting process.
- Consider turning off tagging people in images where possible.

The Don’ts

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

B4 School policy - Online safety group terms of reference

1. PURPOSE

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

2. MEMBERSHIP

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

The composition of the group should include:

- Senior Leadership Team (SLT) member/s
- safeguarding officer
- teaching staff member
- support staff member
- online safety co-ordinator (not ICT coordinator by default)
- governor
- technical support staff (where possible)
- pupil representation – for advice and feedback. Pupil voice is essential in the make-up of the online safety group, but pupils would only be expected to take part in meetings where deemed relevant.

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

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

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

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

3. CHAIRPERSON

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

- scheduling meetings and notifying group members
- inviting other people to attend meetings when required by the group
- guiding the meeting according to the agenda and time available
- ensuring all discussion items end with a decision, action or definite outcome
- making sure that notes are taken at the meetings and that these with any action points are distributed as necessary.

4. FREQUENCY OF MEETINGS

Meetings shall be held Termly. A special or extraordinary meeting may be called when and if deemed necessary.

5. FUNCTIONS

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

- to keep up to date with new developments in the area of online safety
- to (at least) annually review and develop the online safety policy in line with new technologies and incidents
- to monitor the delivery and impact of the online safety policy
- to monitor the log of reported online safety incidents (anonymous) to inform future areas of teaching/learning/training.
- to co-ordinate consultation with the whole school community to ensure stakeholders are up to date with information, training and/or developments in the area of online safety. This could be carried out through:
    - staff meetings

  - pupil forums (for advice and feedback)
  - governors meetings
  - surveys/questionnaires for pupils, parents/carers and staff
  - parents evenings
  - website/learning platform/newsletters
  - online safety events
  - Internet Safety Day (annually held on the second Tuesday in February)
  - other methods
- to ensure that monitoring is carried out of Internet sites used across the school (if possible)
- to monitor filtering/change control logs (e.g. requests for blocking/unblocking sites)
- to monitor the safe use of data across the school
- to monitor incidents involving online bullying for staff and pupils.

6. AMENDMENTS

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

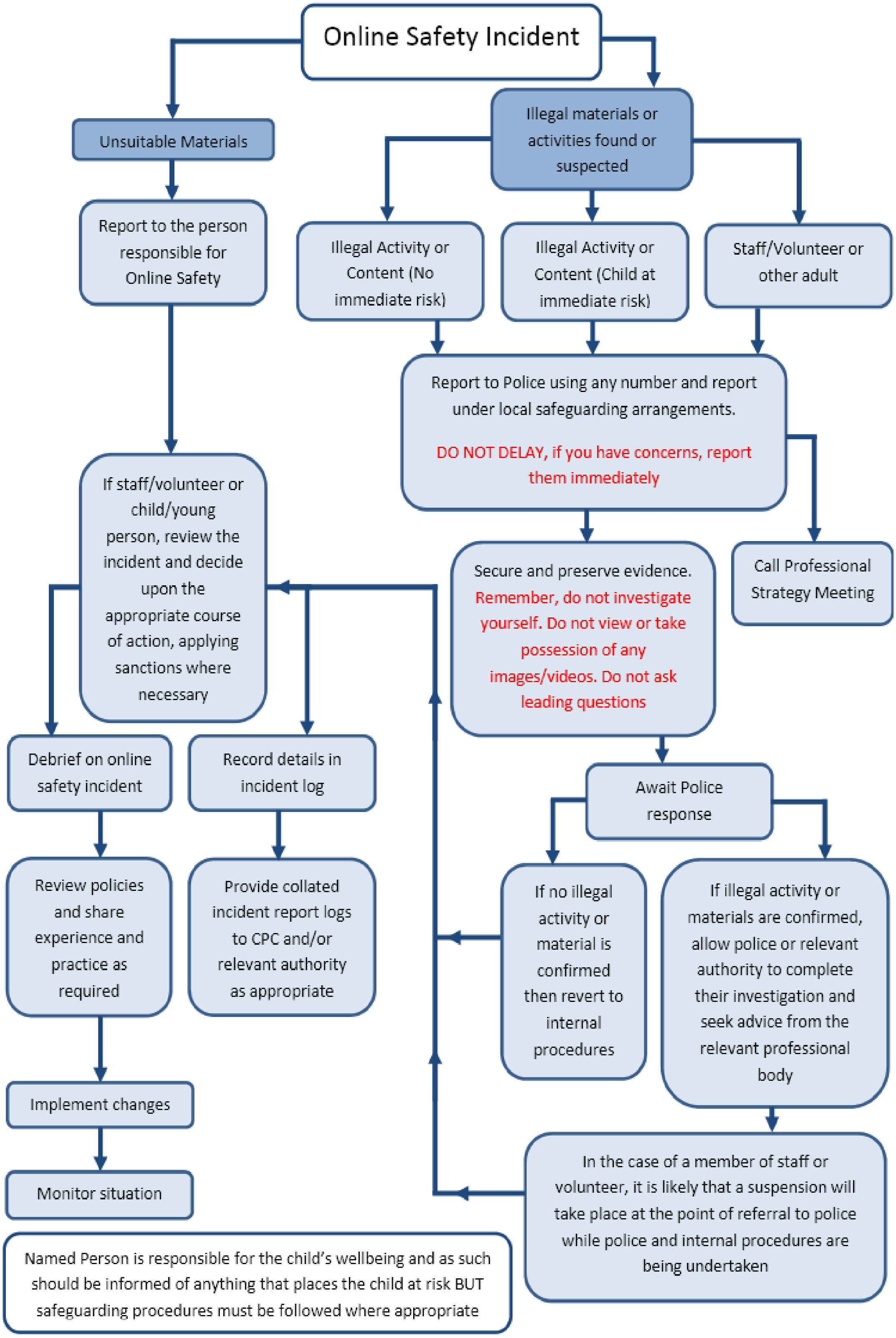
The above Terms of Reference for Ribblesdale High School have been agreed

Reviewed by Governing Board

Date: 9th March 2023

Date for review: March 24

C1 Responding to incidents of misuse – flow chart


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