Blagdon Primary School

Online Safety

Policy

Reviewed by	Jenny Campbell	February 2023
Approved by	Chris Mills	February 2023
Endorsed by	Local Governing Body (LGB)	March 2023
Next Reviewed:	February 2024	

Development / Monitoring / Review of this Policy

This Online Safety policy has been developed by a committee made up of:

- Headteacher/ Senior Leaders
- Online Safety Coordinator
- All Staff – including Teachers, Support Staff, Admin and site staff
- Governors

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

Schedule for Development / Monitoring / Review

This Online Safety policy was approved by the Board of Directors / Governing Body / Governors Sub Committee on:	*March 2023*
The implementation of this Online Safety policy will be monitored by the:	*Headteacher* *E-Safety Leader*
Monitoring will take place at regular intervals:	*Annually*
Governing Body will receive a report on the implementation of the Online Safety Policy generated by the monitoring group (which will include anonymous details of online safety incidents) at regular intervals:	*Annually*
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:	*February 2024*
Should serious online safety incidents take place, the following external persons / agencies should be informed:	*Somerset Multi Agency Safeguarding Hub (Southern MASH), Police, SWGFL, LSP Safeguarding Team dependant on the specifics of the incident.*

The school will monitor the impact of the policy using:

- Logs of reported incidents
- Monitoring logs of internet activity (including sites visited) / filtering available through school technician
- Surveys / questionnaires of
    - pupils
    - parent /carers

Scope of the Policy

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

The Education and Inspections Act 2006 empowers Headteachers / Principals to such extent as is reasonable, to regulate the behaviour of students / pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of online-bullying or other Online Safety incidents covered by this policy, which may take place outside of the school, but is linked to membership of the school. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data. In the case of both acts, action can only be taken over issues covered by the published Behaviour Policy.

Blagdon Primary School will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents / carers of incidents of inappropriate Online Safety behaviour that take place out of school.

Roles and Responsibilities

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

Governors

Governors are responsible for the approval of the Online Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the Governors receiving regular information about online safety incidents and monitoring reports. A member of the Governing Body has taken on the role of Online Safety Governor as part of their duty as Child Protection / Safeguarding Governor. The role of the Online Safety Governor will include:

- regular meetings with the Online Safety Co-ordinator
- regular monitoring of online safety incident logs
- regular monitoring of filtering / change control logs
- reporting to relevant Governors 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 will be delegated to the Online Safety Lead.

- 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 (see flow chart on dealing with online safety incidents – included in a later section – "Responding to incidents of misuse" and relevant *MAT* disciplinary procedures).
- The Headteacher/ Senior Leaders are responsible for ensuring that the Online Safety Lead and other relevant staff receive suitable training to enable them to carry out their online safety roles and to train other colleagues, as relevant.
- The Headteacher/ Senior Leaders will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal online safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.
- The Senior Leadership Team will receive regular monitoring reports from the Online Safety Lead.

Online Safety Lead

- 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 training and advice for staff
- liaises with the MAT
- liaises with school technical staff
- receives reports of online safety incidents and creates a log of incidents to inform future online safety developments
- meets regularly with Online Safety *Governor* to discuss current issues, review incident logs and filtering / change control logs
- attends relevant meeting of *Governors*
- reports regularly to Senior Leadership Team

Technical Staff:

The Technical Staff is responsible for ensuring:

- that the school's technical infrastructure is secure and is not open to misuse or malicious attack
- that Blagdon Primary School meets required online safety technical requirements and any *MAT* Online Safety Policy / Guidance that may apply.
- that users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed
- the filtering policy (if it has one), is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person
- that they keep up to date with online safety technical information in order to effectively carry out their online safety role and to inform and update others as relevant

- that the use of the network is regularly monitored in order that any misuse / attempted misuse can be reported to the Headteacher and/or Online Safety Lead for investigation / action / sanction
- that monitoring software / systems are implemented and updated as agreed in school policies

Teaching and Support Staff

Are responsible for ensuring that:

- they have an up to date awareness of online safety matters and of the current school Online Safety Policy and practices
- they have read, understood and signed the Staff Acceptable Use Policy / Agreement (AUP)
- they report any suspected misuse or problem to the Headteacher/ Senior Leader and/or Online Safety Lead for investigation / action / sanction
- all digital communications with pupils / parents / 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 Policy and acceptable use policies
- pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- they monitor the use of digital technologies, mobile devices, cameras etc in lessons and other school activities (where allowed) and implement current policies with regard to these devices
- in lessons where internet use is pre-planned students should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches

Designated Safeguarding Lead

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

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

Online Safety Group

The Safeguarding Leads act as the Online Safety Group provides a consultative group that has wide representation from Blagdon Primary School community, with responsibility for issues regarding online

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

Members of the Online Safety Group will assist the Online Safety Lead (or other relevant person, as above) with:

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

Pupils:

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

Parents / Carers

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

- digital and video images taken at school events
- access to parents' sections of the website

- their children's personal devices in Blagdon Primary School (where this is allowed)

Community Users

Community Users who access school systems Platform as part of the wider *school* provision will be expected to sign a Community User AUA before being provided with access to school systems.

Policy Statements

Education – Pupils

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

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

- A planned online safety curriculum should be provided as part of Computing / PHSE / other lessons and should be regularly revisited
- Key online safety messages should be reinforced as part of a planned programme of assemblies and pastoral activities
- Pupils should be taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information.
- 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 student / pupil Acceptable Use Agreement and encouraged to adopt safe and responsible use both within and outside school.
- Staff should act as good role models in their use of digital technologies, the internet and mobile devices
- In lessons where internet use is pre-planned, it is best practice that 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.
- Where pupils are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit.

- It is accepted that from time to time, for good educational reasons, students may need to research topics (eg racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Technical Staff (or other relevant designated person) can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need.

Education – Parents / Carers

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

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

- Curriculum activities
- Letters, newsletters, the school website
- Parents / Carers evenings / sessions
- High profile events / campaigns e.g. Safer Internet Day
- Reference to the relevant websites / publications e.g. Digital Parenting, swgfl.org.uk www.saferinternet.org.uk/ http://www.childnet.com/parents-and-carers

Education – The Wider Community

Blagdon Primary 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.
- Blagdon Primary School website will provide online safety information for the wider community
- Supporting community groups e.g. Early Years Settings, Childminders, youth / sports / voluntary groups to enhance their Online Safety provision

Education & Training – Staff / Volunteers

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

- A planned programme of formal online safety training will be made available to staff. This will be regularly updated and reinforced. An audit of the online safety training needs of all staff will be carried out regularly.
- All new staff should receive online safety training as part of their induction programme, ensuring that they fully understand Blagdon Primary School Online Safety Policy and Acceptable Use Agreements.
- It is expected that some staff will identify online safety as a training need within the performance management process.
- The Online Safety Lead (or other nominated person) will receive regular updates through attendance at external training events (eg from SWGfL / LA/ LSP / 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 meetings / INSET days.
- The Online Safety Lead (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 subcommittee / group involved in technology / online safety / health and safety /safeguarding. This may be offered in a number of ways:

- Attendance at training provided by the MAT or other relevant organisation (e.g. SWGfL).
- Participation in school training / information sessions for staff or parents

Technical – infrastructure / equipment, filtering and monitoring

Blagdon Primary 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 Blagdon Primary School meets recommended technical requirements
- There will be regular reviews and audits of the safety and security of school technical systems
- Servers, wireless systems and cabling must be securely located and physical access restricted
- All users will have clearly defined access rights to school technical systems and devices.
- All users (at KS2) will be provided with a username and secure password by the Online Safety Lead and Network Manager who will keep an up to date record of users and their usernames. Users are responsible for the security of their username and password and will be required to change their password every six weeks.

- The administrator passwords for Blagdon Primary School ICT systems, used by the Network Manager must also be available to the Headteacher or other nominated senior leader and kept in a secure place (eg school safe).
- The School technical staff are responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations.
- Internet access is filtered for all users. Illegal content (child sexual abuse images) is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list. Content lists are regularly updated and internet use is logged and regularly monitored. There is a clear process in place to deal with requests for filtering changes
- Internet filtering / monitoring should ensure that children are safe from terrorist and extremist material when accessing the internet.
- Blagdon Primary School has provided enhanced / differentiated user-level filtering
- School technical staff regularly monitor and record the activity of users on the school technical systems and users are made aware of this in the Acceptable Use Agreement.
- An appropriate system is in place for users to report any actual / potential technical incident / security breach to the relevant person, as agreed).
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, mobile devices etc from accidental or malicious attempts which might threaten the security of the school systems and data. These are tested regularly. The school infrastructure and individual workstations are protected by up to date virus software.
- The Acceptable Use Policy Agreement is in place regarding the extent of personal use that users (staff / students / pupils / community users) and their family members are allowed on school devices that may be used out of school.
- An agreed policy is in place that restricts staff from downloading executable files and installing programmes on school devices.
- An agreed policy is in place regarding the use of removable media (eg memory sticks / CDs / DVDs) by users on school devices. Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured.

Mobile Technologies (including BYOD/BYOT)

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

All users should understand that the primary purpose of the use mobile / personal devices in a school context is educational. The mobile technologies policy should be consistent with and inter-related to other relevant school polices including but not limited to the Safeguarding Policy, Behaviour Policy, Bullying Policy, Acceptable Use Policy, and policies around theft or malicious damage. Teaching about the safe and

appropriate use of mobile technologies should be an integral part of the school's Online Safety education programme.

The school Acceptable Use Policy Agreements for staff and parents/carers/ visitors will give consideration to the use of mobile technologies

Where BYOD is granted, the school expects users to act responsibly, safely and respectfully in line with current Acceptable Use Policy Agreements, in addition;

- Devices are brought into school at the owner's risk
- Visitors should be provided with information about how and when they are permitted to use mobile technology in line with local safeguarding arrangements
- 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 school.
- Devices must be in silent mode on the school site
- Devices brought into school are provided to support learning.
- Confiscation and searching (England) - the school has the right to take, examine and search any device that is suspected of unauthorised use, either technical or inappropriate.
- 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 to work is not permitted
- The software / apps originally installed by the school must remain on the school owned device in usable condition and be easily accessible at all times. From time to time the school may add software applications for use in a particular lesson. Periodic checks of devices will be made to ensure that users have not removed required apps
- Users must only photograph people with their permission. Users must only take pictures or videos that are required for a task or activity. All unnecessary images or videos will be deleted immediately
- Staff owned devices should not be used for personal purposes during teaching sessions, unless in exceptional circumstances
- Printing from personal devices will not be possible

The school allows:

	School Devices			Personal Devices		
	School owned for single user	School owned for multiple users	Authorised device[1]	Student owned with permission	Staff owned	Visitor owned

[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.

Allowed in school	*Yes*	*Yes*	*Yes*	*Yes but not to be used and stored safely*	*Yes but not used in presence of children*	*Yes but not used*
Full network access	*Yes*	*Yes*	*Yes*			
Internet only					*Yes*	*Yes for Governors and education al visitors*
No network access				*Yes*		*Yes – to other visitors*

Use of digital and video images

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

- When using digital images, staff should inform and educate students about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.
- Written permission from parents or carers will be obtained before photographs of students / pupils are published on the school website / social media / local press
- 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 or members of staff 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 students / pupils are appropriately dressed and are not participating in activities that might bring the individuals or Portishead Primary School into disrepute.
- Students / pupils must not take, use, share, publish or distribute images of others without their permission
- Photographs published on the website, or elsewhere that include students / pupils will be selected carefully and will comply with good practice guidance on the use of such images.
- Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs.
- Pupils' work can only be published with the permission of the pupil and parents or carers.

Data Protection

See Data Protection Policy

Communications

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

	Staff & other adults			Pupils				
Communication Technologies	Allowed	Allowed at certain times	Not allowed	Allowed	Allowed at start and end of day	Allowed at certain times	Allowed with staff permission	Not allowed
Mobile phones may be brought to the school / academy	x				x			
Use of mobile phones in lessons			x					x
Use of mobile phones in social time	x							
Taking photos on mobile phones / cameras			x					x

Use of other mobile devices e.g. tablets, gaming devices		x		x
Use of personal email addresses in school , or on school network	x			x
Use of school email for personal emails		x		x
Use of messaging apps		x		x
Use of social media		x		x
Use of blogs		x		x

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

- The official school email service may be regarded as safe and secure and is monitored. Users should be aware that email communications are monitored. Staff and students / pupils should therefore use only Blagdon Primary School email service to communicate with others when in school, or on school systems (e.g. by remote access).
- Users must immediately report, to the nominated person – in accordance with Blagdon Primary 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 (email, social media, chat, blogs, VLE etc) must be professional in tone and content. These communications may only take place on official (monitored) school systems. Personal email addresses, text messaging or social media must not be used for these communications.
- Whole class / group email addresses may be used at KS1, while students at KS2 will be provided with individual school email addresses for educational use.
- Students should be taught about online safety issues, such as the risks attached to the sharing of personal details. They should also be taught strategies to deal with inappropriate communications and be reminded of the need to communicate appropriately when using digital technologies.
- Personal information should not be posted on Bladon Primary School website and only official email addresses should be used to identify members of staff.

Social Media - Protecting Professional Identity

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

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

- Ensuring that personal information is not published
- Training is provided including: acceptable use; social media risks; checking of settings; data protection; reporting issues.
- Clear reporting guidance, including responsibilities, procedures and sanctions
- Risk assessment, including legal risk

School staff should ensure that:

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

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

- A process for approval by senior leaders
- Clear processes for the administration and monitoring of these accounts – involving at least two members of staff
- A code of behaviour for users of the accounts, including:
    - Systems for reporting and dealing with abuse and misuse
    - Understanding of how incidents may be dealt with under school disciplinary procedures

Personal Use:

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

The school's use of social media for professional purposes will be checked regularly by the senior risk officer and Online Safety Group to ensure compliance with the school policies.

Dealing with unsuitable / inappropriate activities

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

Blagdon Primary School believes that the activities referred to in the following section would be inappropriate in a school context and that users, as defined below, should not engage in these activities in / or outside Portishead Primary School when using school equipment or systems. Blagdon Primary 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,	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

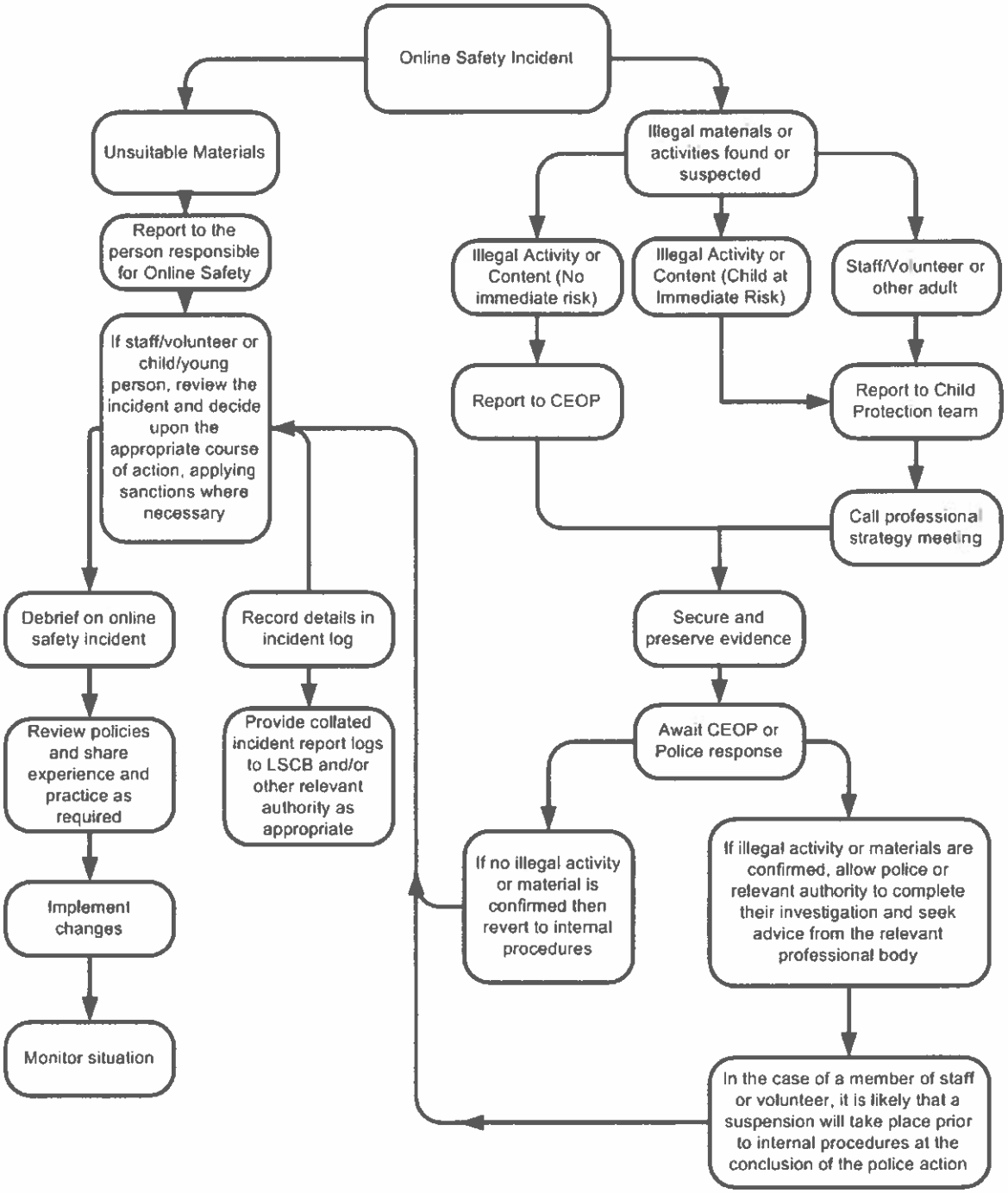
	Criminally racist material in UK – to stir up religious hatred (or hatred on the grounds of sexual orientation) - contrary to the Public Order Act 1986			X
	Pornography		X	
	Promotion of any kind of discrimination		X	
	threatening behaviour, including promotion of physical violence or mental harm			X
	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 / academy			X	
Infringing copyright				X
Revealing or publicising confidential or proprietary information (eg 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	
On-line gaming (educational)		X		
On-line gaming (non-educational)		X		
On-line gambling			X	
On-line shopping / commerce		X		
File sharing			X	
Use of social media		X		
Use of messaging apps		X		
Use of video broadcasting e.g. Youtube		X		

Responding to incidents of misuse

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

Illegal Incidents

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



Other Incidents

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

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

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

School Actions & Sanctions

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

Pupils Incidents	Actions / Sanctions								
	Refer to class teacher	Refer to SLT	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 eg detention / exclusion
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).		x	x	x		x			
Unauthorised use of non-educational sites during lessons	x					x			
Unauthorised / inappropriate use of mobile phone / digital camera / other mobile device		x	x			x			
Unauthorised / inappropriate use of social media / messaging apps / personal email		x	x			x			
Unauthorised downloading or uploading of files		x	x			x			
Allowing others to access school network by sharing username and passwords	x	x	x			x		x	

Attempting to access or accessing Blagdon Primary School network, using another student's / pupil's account	x		x			x		x	
Attempting to access or accessing Blagdon Primary School network, using the account of a member of staff			x		x	x			x
Corrupting or destroying the data of other users	x	x	x			x	x		
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature			x			x		x	x
Continued infringements of the above, following previous warnings or sanctions			x			x			x
Actions which could bring Blagdon Primary 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 / academy'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
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act			x			x			x

Staff Incidents

	Actions / Sanctions							
	Refer to line manager	Refer to Headteacher	Refer to MAT / 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				x
Inappropriate personal use of the internet / social media / personal email		x						
Unauthorised downloading or uploading of files		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		
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		
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software		x	x	x		x		x
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature		x	x					
Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with students / pupils		x						
Actions which could compromise the staff member's professional standing			x			x		
Actions which could bring Blagdon Primary School into disrepute or breach the integrity of the ethos of Blagdon Primary School			x			x		
Using proxy sites or other means to subvert the school's / academy's filtering system			x			x		

Accidentally accessing offensive or pornographic material and failing to report the incident		x	x	
Deliberately accessing or trying to access offensive or pornographic material		x		x
Breaching copyright or licensing regulations	x			
Continued infringements of the above, following previous warnings or sanctions		x		x

In the event of such an incident occurring, a written record would be made describing both the incident and the action taken, together with rationale appropriate. This record will be retained within the individual's personal file and e-safety incident log and safeguarding file as appropriate.

Acknowledgements

SWGfL would like to acknowledge a range of individuals and organisations whose policies, documents, advice and guidance have contributed to the development of this School Online Safety Policy Template and of the 360 degree safe Online Safety Self Review Tool:

- Members of the SWGfL Online Safety Group
- Avon and Somerset Police
- Representatives of SW Local Authorities
- Plymouth University Online Safety
- NEN / Regional Broadband Grids

Appendix

This policy should be read in conjunction with the following policies:

- Mobile Phone Policy (separate)
- Password Policy
- Electronic Devices Search and Deletion Policy

PASSWORD POLICY

Introduction

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, without permission (or as 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 whilst using the system

Responsibilities

The management of the password security policy will be the responsibility of the online safety coordinator, ICT technician and SLT.

All adults and pupils in Key Stage 2 will have responsibility for the security of their username and password. Adults and pupils in KS2 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. In Key Stage 1, class logins will be used but monitored by the relevant class teachers, with any concerns being passed on to the online safety coordinator. Where pupils have login and passwords in KS1 / EYFS have passwords to access online learning (eg via Teams/Apps), these will be given to the parents / carers and the class teacher.

Passwords for new users and replacement passwords for existing users will be allocated by the ICT Lead. Adult users will change their passwords every term, while KS2 pupils will change their passwords every year. All users at KS2 will be provided with a username and password by the ICT Technician who will keep an up to date record of users and their usernames.

The following rules apply to the use of passwords:

- Never reveal your password to anyone
- Do not use any part of your username within the password
- Never write your password down or store them where they are left open
- Passwords shall not be displayed on screen, and shall be securely hashed
- Requests for password changes should be made in person to the online safety coordinator, ensuring that the new password can only be passed to the genuine user.

The following rules apply to the use of passwords for adults:

- Passwords must be changed every term.
- Adult passwords should be a minimum of 8 characters long and must include three of – uppercase character, lowercase character and number.
- Computers and laptops will be screen locked when leaving a room.
- The "administrator" passwords for the school ICT system, used by the ICT technician and online safety coordinator must also be available to the Headteacher or other nominated senior leader and kept in a secure place.
-

Training / Awareness

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

- At induction.
- Through this policy.
- Through the Acceptable Use Policy Statement.

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

- In computing, PSHE or E-safety lessons.
- Through the Acceptable Internet Use Statement.

Electronic Devices - Search & Deletion Policy

Introduction

In response of the changing face of information technologies and increasing pupil use of these technologies, Part 2 of the Education Act 2011 (Discipline) has introduced new powers to schools to search pupils for items 'banned under the school rules' where necessary in order to maintain discipline and ensure safety. This includes the power to 'delete data' stored on seized electronic devices.

Pupils are discouraged from bringing mobile phones or other personal electronic devices to school other than with prior permission in specific circumstances. They must only be used within the rules laid down by the school. Items banned under the school rules are determined and publicised by the Headteacher (section 89 Education and Inspections Act 1996).

An authorised member of staff finding an electronic device may access and examine any data or files on the device if they think there is a good reason to do so (i.e. the staff member must reasonably suspect that the data or file on the device in question has been, or could be, used to cause harm, to disrupt teaching or break the school rules).

Authorised staff (have the right to;

- Search with consent - Authorised staff may search with the pupil's consent for any item.
- Search without consent - Authorised staff may only search without the pupil's consent for anything which is either 'prohibited' (as defined in Section 550AA of the Education Act 1996) or appears in the school rules as an item which is banned and may be searched for
- Staff must have reasonable grounds for suspecting that a pupil is in possession of a prohibited item i.e. an item banned by the school rules and which can be searched for.
- Staff should take reasonable steps to check the ownership of the mobile phone / personal electronic device before carrying out a search. (The powers included in the Education Act do not extend to devices owned (or mislaid) by other parties e.g. a visiting parent or contractor
- Where possible, searches should not take place in public places e.g. an occupied classroom, which might be considered as exploiting the pupil being searched.
- Staff carrying out the search must be the same gender as the pupil being searched; and there must be a witness (also a staff member), where possible they too should be the same gender as the pupil being searched.
- There is an exemption whereby authorised staff can carry out a search of a pupil of the opposite gender including without a witness present, when they reasonably believe that there is a risk that serious harm will be caused to a person if the search is not conducted immediately and it is not reasonably practicable to summon another member of staff.
- The person conducting the search may not require the pupil to remove any clothing other than outer clothing, i.e. hats; shoes; boots; coat; blazer; jacket; gloves and scarves).

- A pupil's possessions can only be searched in the presence of the pupil and another member of staff, except where there is a risk that serious harm will be caused to a person if the search is not conducted immediately and where it is not reasonably practicable to summon another member of staff.
- "Possessions" means any goods over which the pupil has or appears to have control – this includes desks, lockers and bags.

Force cannot be used to search without consent for items banned under the school rules regardless of whether the rules say an item can be searched for.

Electronic Devices

The examination of the data / files on the device should go only as far as is reasonably necessary to establish the facts of the incident. Any further intrusive examination of personal data may leave the school open to legal challenge. It is important that authorised staff should have training and sufficient knowledge of electronic devices and data storage. If inappropriate material is found on the device it is up to the authorised member of staff to decide whether they should delete that material, retain it as evidence (of a criminal offence or a breach of school discipline) or whether the material is of such seriousness that it requires the involvement of the police. Examples of illegal activity would include:

- child sexual abuse images (including images of one child held by another child)
- adult material which potentially breaches the Obscene Publications Act
- criminally racist material
- other criminal conduct, activity or material.

Following an examination, the device may be returned to the owner, retained or dispose of, the authorised staff member may erase any data or files, if they think there is a good reason to do so. Specific training is required for those staff who may need to judge whether material that is accessed is inappropriate or illegal.

Members of staff may require support in judging whether the material is inappropriate or illegal. One or more Senior Leaders should receive additional training to assist with these decisions. Care should be taken not to delete material that might be required in a potential criminal investigation.

The school should also consider their duty of care responsibility in relation to those staff who may access disturbing images or other inappropriate material whilst undertaking a search. There should be arrangements in place to support such staff.

The responsible person, school E Safety lead, will ensure that full records are kept of incidents involving the searching for and of mobile phones and electronic devices and the deletion of data / files. These records will be reviewed by ESafety lead, Designated Safeguarding lead or Deputy and E-Safety Governor three times a year or more where necessary). This policy will be reviewed by the Headteacher and governors annually and in response to changes in DfE guidance. More detailed information regarding the

Education Act 2011 can be found in "Screening, searching and confiscation – Advice for head teachers, governors and governing bodies.

http://www.education.gov.uk/schools/pupilsupport/behaviour/behaviourpolicies/f0076897/screening-searching-andconfiscation