BROAD HINTON CHURCH OF ENGLAND PRIMARY SCHOOL

'A Love of Learning for a Lifetime of Opportunities'

'At Broad Hinton School we are proud of our educational heritage, which is rooted historically in Christian Belief. We aim to provide opportunities for all to learn and achieve within a happy, structured and disciplined Christian environment.
We welcome everyone to our village school where all faiths, cultures and abilities are received with love, care and respect.'

ONLINE SAFETY POLICY

Our Online safety Policy has been written by the school, building template policy from SWGfL and latest government guidance. It has been agreed by the Head teacher and approved by the governors. It will be reviewed annually or more regularly if necessary.

The school will monitor the impact of the policy using

- Logs of reported incidents
- Curriculum overviews of coverage and content
- Surveys/questionnaires of pupils, staff, parents and link governor for computing and safeguarding

Schools' Online Safety Policy

Wiltshire Council believes in the educational benefits of Digital Technology for effective teaching and learning practices. Secure and effective internet access for pupils should be seen as an entitlement based on educational need and an essential resource for staff. Management that recognises the online safety issues and plans accordingly will help to ensure appropriate, effective and safe use by all.

Related Policies and Guidance

This policy should be read alongside the school's Child Protection and Safeguarding Policy, Staff Behaviour Policy (Code of Conduct), Behaviour Policy, Acceptable Use Agreements, Data Protection Policy and the current version of Keeping Children Safe in Education (KCSIE).

This policy applies to all members of the school community (including staff, students/pupils, volunteers, parents/carers, visitors, community users) who have access to and are users of school digital technology systems, both in and out of the school.
The Education and Inspections Act 2006 empowers Headteachers/Principals to such extent as is reasonable, to regulate the behaviour of 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.
The school will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents/carers of incidents of inappropriate online safety behaviour that take place out of school.

Roles and Responsibilities
The following section outlines the online safety roles and responsibilities of individuals and groups within the school:
Governors
Governors 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 The role of the Online Safety Governor will include:

- regular meetings with the Online Safety/Computing subject lead
- regular monitoring of any online safety incident logs
- regular discussions of filtering/change control logs
- reporting to relevant Governors Curriculum meeting

Headteacher/Principal 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 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 and will be responded to by the Designated Safeguarding Lead using the Wiltshire flowchart of 'Allegations of adults in education settings'.
- The Headteacher and all staff are responsible for ensuring that all staff receive suitable training to enable them to carry out their online safety roles; see the online safeguarding training; Online Safety INSET Presentation | Childnet and/or via Flick Learning
- The Headteacher will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal online safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles. Monitoring may include: pupil voice sessions, questionnaires and in class discussions.

Online Safety Lead
The online safety lead in Broad Hinton Primary School is also the Designated Safeguarding Lead Children are taught about safeguarding, including online safety. Online safety is considered as part of our whole school safeguarding approach and wider staff training and curriculum planning. A personalised and contextualised approach is taken for vulnerable children, including those with SEND, communication difficulties, social and emotional needs, safeguarding concerns or limited access to appropriate supervision online. Additional support and risk assessment may be implemented where required.
They will:

- take on the day to day responsibility for online safety issues (alongside school staff) 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; see child protection policy for recording instances.
- provides training and advice for staff
- liaises with the Local Authority when necessary or appropriate
- liaises with school technical contractors; 123ICT
- receives reports of online safety incidents and creates a log of incidents to inform future online safety developments; see Appendix
- meets regularly with Online Safety/Safeguarding *Governor* to discuss current issues, review incident logs and filtering/change control logs
- attends relevant meetings of *Governors*
- reports regularly to Senior Leadership Team

Technical staff/contractor (123ICT)

Broad Hinton Primary School has a managed ICT service provided by an outside contractor, it is therefore the responsibility of the school to ensure that the managed service provider carries out all the online safety measures that would otherwise be the responsibility of the school technical staff, as suggested below. It is also important that the managed service provider is fully aware of the school online safety policy and procedures.

Those with technical responsibilities are responsible for ensuring:

- that the school's technical infrastructure is secure and is not open to misuse or malicious attack
- that the school meets required online safety technical requirements and any Local Authority online safety policy/guidance that may apply.
- that users may only access the networks and devices through a properly enforced password protection policy
- the filtering policy 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 networks/internet/digital technologies is regularly monitored in order that any misuse/attempted misuse can be reported to the Headteacher and Online Safety Lead for investigation/action/sanction
- that monitoring software/systems are implemented and updated as agreed in school/academy 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 behaviour policy
- they report any suspected misuse or problem to the Headteacher and Online Safety Lead for investigation/action/sanction
- all digital communications with students/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

- students/pupils understand and follow the Online Safety Policy policy
- students/pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- they monitor the use of digital technologies, mobile devices, cameras, etc. in lessons and other school activities (where allowed) and implement current policies with regard to these devices
- in lessons where internet use is pre-planned students/pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches

Designated Safeguarding Lead

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
- exposure to harmful online challenges and trends
- misinformation and disinformation
- AI-generated and manipulated content (deepfakes)
- financial exploitation and online scams
- risks associated with gaming platforms, livestreaming and private messaging services

Students/Pupils:

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

Parents/carers

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

- digital and video images taken at school events
- access to parents' sections of the website, learning platforms eg: SeeSaw and the school Facebook page

Education – Students/Pupils

Internet access for pupils should be seen as an entitlement on the basis of educational need and an essential resource for staff. Parental permission should be sought at least at the start of each Key Stage.

- The school receives Internet Service Provision (ISP) from South West Grid for Learning (SWGfL) and has a service which proactively monitors Internet usage for attempts to access illegal (child abuse and incitement for racial hatred) content and will notify the local police and Wiltshire Council in these instances.
- The school receives Internet Service Provision (ISP) from South West Grid for Learning (SWGfL) and will request monitoring reports from the ISP which will be regularly checked to identify any attempts to access illegal content and should notify the local police and Wiltshire Council in these instances.

Whilst 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/digital literacy 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.

In planning their online safety curriculum schools/academies may wish to refer to:

- SWGfL Project Evolve – online safety curriculum programme and resources
- NSPCC website
- Childnet website
- CEOP Think you know website

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 or on the national Safer Internet Day
- 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 understand the benefits and risks of Artificial Intelligence (AI) tools. They should learn that information and images generated by AI may not always be accurate, appropriate or unbiased and should be critically evaluated before use.
- 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

- 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 (e.g. racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Technical Staff (or other relevant designated person) can temporarily remove those sites from the filtered list for the period of study.

Education – Parents/carers

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

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

- Curriculum activities
- Letters, newsletters, learning platform eg: SeeSaw
- Parents/carers online safety sessions
- High profile events/campaigns e.g. Safer Internet Day
- Reference to the relevant web sites/publications found on our school safeguarding page
- Regular updates about emerging online risks, parental controls, gaming platforms, social media trends and AI technologies.

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:

- 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
- Sharing their online safety expertise/good practice with other local schools
- 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. Staff Led Online Safety INSET Presentation | Childnet and/or via Flick Learning
- 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 staff behaviour policy

- The Online Safety Lead (or other nominated person) will provide advice/guidance/training to individuals as required.
- Staff will receive guidance on the safe and appropriate use of AI technologies. Confidential, safeguarding or personal information must not be entered into public AI systems unless approved by the school and compliant with data protection requirements.

Training – Governors

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

- Participation in school training/information sessions for staff or parents (this may include attendance at assemblies/lessons).

Technical – infrastructure/equipment, filtering and monitoring

Broad Hinton Primary School has a managed ICT service provided by an outside contractor, 123ICT, and it is the responsibility of the school to ensure that the managed service provider carries out all the online safety measures that would otherwise be the responsibility of the school, as suggested below. It is also important that the managed service provider is fully aware of the school online safety policy. The school and managed service should also check their Local Authority on these technical issues.

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 by the managed ICT provider
- Servers, wireless systems and cabling must be securely located and physical access restricted
- All users will have clearly defined access rights to school technical systems and devices.
- All users will be provided with a username and secure password by our managed provider 123ICT who will keep an up-to-date record of users and their usernames. Users are responsible for the security of their username and password.
- The "master/administrator" passwords for the school systems, used by the Network Manager (or other person) must also be available to the Headteacher and administrative officer.
- Our managed provider, 123 ICT, is responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations
- Internet access is filtered for all users. Illegal content (child sexual abuse images) is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list. Content lists are regularly updated and internet use is logged and regularly monitored. There is a clear process in place to deal with requests for filtering changes

- Filtering and monitoring systems will be reviewed regularly by school leaders and the governing body to ensure they remain effective and appropriate for the age and needs of pupils. Records of monitoring reviews will be maintained.
- Internet filtering/monitoring should ensure that children are safe from terrorist and extremist material when accessing the internet. N.B. additional duties for schools under the Counter Terrorism and Securities Act 2015 which requires schools/academies to ensure that children are safe from terrorist and extremist material on the internet.
- An appropriate system is in place for those using CPOMS for users to report any actual/potential technical incident/security breach to the relevant person, as agreed. If an pupil sees any material on a device that is disturbing and making them feel uncomfortable or is inappropriate, they are taught to tell an adult immediately. The adult will then alert the Designated Safeguarding Lead so it can be dealt with accordingly.
- 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 devices are protected by up-to-date virus software.
- Each teacher is given access to mobile devices in school which are to be purely used for teaching and learning. These devices should not leave the site unless the device is being used at home for work purposes. The mobile device should be returned the next working day. Teaching staff are not to install APPS or programmes without consent from the headteacher. 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. If the school decide to lend a family a mobile device for home learning it will be the parent's responsibility to ensure correct use and careful filtering of online websites and networks. When the device is returned the history will be checked before any other child is allowed to use it.

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.

In preparing a mobile technologies policy the school should consider possible issues and risks. These may include: security risks in allowing connections to your school network, filtering of personal devices, breakages and insurance, access to devices for all students, avoiding potential classroom distraction, network connection speeds, types of devices, charging facilities, total cost of ownership. A range of mobile technology implementations is possible

A checklist of points to be considered in included below.

- **The school allows:** (the school should complete the table below to indicate which devices are allowed and define their access to school systems)

	School Devices; ipads, laptops, cameras			Personal Devices		
	School owned for single user	**School owned for multiple users**	**Authorised device[1]**	**Student /family owned**	**Staff owned**	**Visitor owned**
Allowed in school	*Yes*	*Yes*	*Yes*	*No*	*Yes*	*No*
Full network access	*Yes*	*Yes*	*Yes*	*No*	*No*	*No*

School owned/provided devices:
Each class is allocated an ipad and laptop for the teachers use. All other ipads and laptops/chromebooks are for general use by the children and teaching assistants in their work and teaching and learning support.
Teaching staff can take their mobile devices home for teaching and learning reasons only and will be returned the next working day. Installation of APPs and programmes on any device needs to be authorized by the headteacher and then our managed provider will install accordingly using our security logins. Regular review of photographs and videos will be conducted by the teachers and removal of unnecessary items will be conducted. Broad Hinton Primary School is committed to training their staff in ICT and thus will provide this according to need. The mobile devices will be returned to the headteacher when a member of staff leaves or when on long term sick so it can be used by other members of staff. The Cloud facility is used to store teaching tools and resources and this is managed by our provider 123ICT.

Personal devices:
All staff in school are able to bring in their mobile phones for personal reasons which may be used at break time or lunchtime or any time outside school hours. In school hours the mobile phone must be kept in a handbag or cupboard which allows it to be safe and away from children and use around children. When visitors arrive in school, they are asked not to use their mobile phones unless they request from the headteacher. On school trips the staff will have their phone available for any contact with school, whether it be a check in from the headteacher, details of returning to inform families or in an emergency. Mobile phone numbers will not be shared with parents attending trips. If any child is permitted to bring a mobile phone or tracking device into school for the purposes of walking home from school, the device should be given to the class teacher or office, where it will be placed in a locked drawer ready to return to the child at the end of the school day.

Use of digital and video images
The development of digital imaging technologies has created significant benefits to learning, allowing staff and students/pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents/carers and 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

[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.

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.
- 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 students/pupils in the digital/video images. All parents on entry to the school and annually after that will be asked to sign a consent for internet use and use of photographs and videos.
- Staff and volunteers are allowed to take digital/video images to support educational aims, but must follow only publish them on our learning platforms; SeeSaw and DBPrimary, which have full security measures in place. 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' names will not be used anywhere on a website or blog, particularly in association with photographs.
- Pupil's work can only be published with the permission of the student/pupil and parents or carers.

Data Protection

With effect from 25th May 2018, the data protection arrangements for the UK changed following the European Union General Data Protection Regulation (GDPR). As a result, schools are likely to be subject to greater scrutiny in their care and use of personal data. Personal data will be recorded, processed, transferred and made available according to the current data protection legislation.

The school/academy must ensure that:

- it has a Data Protection Policy.
- it implements the data protection principles and is able to demonstrate that it does so through use of policies, notices and records (see school website for associated documents)
- 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 'Data ecosystem' in place and knows exactly what personal data it holds, where this data is held, why and which member of staff has responsibility for managing it
- the information asset register records the lawful basis for processing personal data (including, where relevant, how consent was obtained and refreshed). Where special category data is processed, an additional lawful basis will have also been recorded
- it will hold only the minimum personal data necessary to enable it to perform its function and it will not hold it for longer than necessary for the purposes it was collected for. The school should develop a document (Data Ecosystem) to outline how long to keep documents and to ensure there are clear and understood policies and routines for the deletion and disposal of data to support this. personal data held must be accurate and up to date where this is necessary for the purpose it is processed for. Have systems in place to identify inaccuracies, such as asking parents to check emergency contact details at suitable intervals

- it provides staff, parents, volunteers, teenagers and older children with information about how the school looks after their data and what their rights are in a clear Privacy Notice
- procedures must be in place to deal with the individual rights of the data subject, e.g. one of the 8 data subject rights applicable is that of Subject Access which enables an individual to see to have a copy of the personal data held about them
- IT system security is ensured and regularly checked. Patches and other security essential updates are applied promptly to protect the personal data on the systems. Administrative systems are securely ring fenced from systems accessible in the classroom/to learners
- it has undertaken appropriate due diligence and has required data processing clauses in contracts in place with any data processors where personal data is processed.
- it understands how to share data lawfully and safely with other relevant data controllers.
- it reports any relevant breaches to the Information Commissioner within 72hrs of becoming aware of the breach in accordance with UK data protection 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 (see the school website)

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

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

Staff must ensure that they:

- at all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse

- can recognise a possible breach, understand the need for urgency and know who to report it to within the school
- can help data subjects understands their rights and know how to handle a request whether verbal or written. Know who to pass it to in the school
- where personal data is stored or transferred on mobile or other devices (including USBs) these must be encrypted and password protected.
- will not transfer any school/academy personal data to personal devices except as in line with school policy
- access personal data sources and records only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data

Communications

A wide range of rapidly developing communications technologies has the potential to enhance learning.

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

- The official school email service may be regarded as safe and secure and is monitored. Users should be aware that email communications are monitored.
- Users must immediately report, to any adult in school– 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 must be professional in tone and content and use the school systems. Personal email addresses, text messaging or social media must not be used for these communications.
- Whole class email addresses may be used at KS1 and Year 3 and 4, while pupils in Year 5 and 6 will be provided with individual school email addresses for educational use via DBPrimary Learning Platform.
- Pupils should be taught about online safety issues, such as the risks attached to the sharing of personal details. They should also be taught strategies to deal with inappropriate communications and be reminded of the need to communicate appropriately when using digital technologies.
- Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff.

Social Media - Protecting Professional Identity

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

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

- Ensuring that personal information is not published
- Training is provided including: acceptable use; social media risks; checking of settings; data protection; reporting issues; https://www.childnet.com/teachers-and-

professionals/staff-led-onlinonline safety-presentations-/staff-led-onlinonline safety-inset-presentation

- Clear reporting guidance, including responsibilities, procedures and sanctions
- Risk assessment, including legal risk

School/academy 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 local authority
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information
- Staff should take reasonable steps to ensure that AI-generated content, photographs or media shared online do not identify pupils, compromise confidentiality or damage professional standards.

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

- A process for approval by the headteacher
- Clear processes for the administration and monitoring of these accounts – involving at least two members of staff; headteacher and administrative officer
- A code of behaviour for users of the accounts, including
- Systems for reporting and dealing with abuse and misuse and the understanding of how incidents may be dealt with under school disciplinary procedures under the safeguarding and child protection remit.

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 the school or impacts on the school, it must be made understood that the member of staff is not communicating on behalf of the school. 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

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
- The school's use of social media for professional purposes will be checked regularly by the headteacher 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 context, either because of the age of the users or the nature of those activities. The school believes that the activities referred to in the following section would be inappropriate in a school context and that users, as defined below, should not engage in

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

User Actions		Acceptable	Acceptable at certain times	Acceptable for nominated	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	
Activities that might be classed as cyber-crime under the Computer Misuse Act: • Gaining unauthorised access to school networks, data and files, through the use of computers/devices • Creating or propagating computer viruses or other harmful files • Revealing or publicising confidential or proprietary information (e.g. financial / personal information, databases, computer / network access codes and passwords) • Disable/Impair/Disrupt network functionality through the use of computers/devices						X

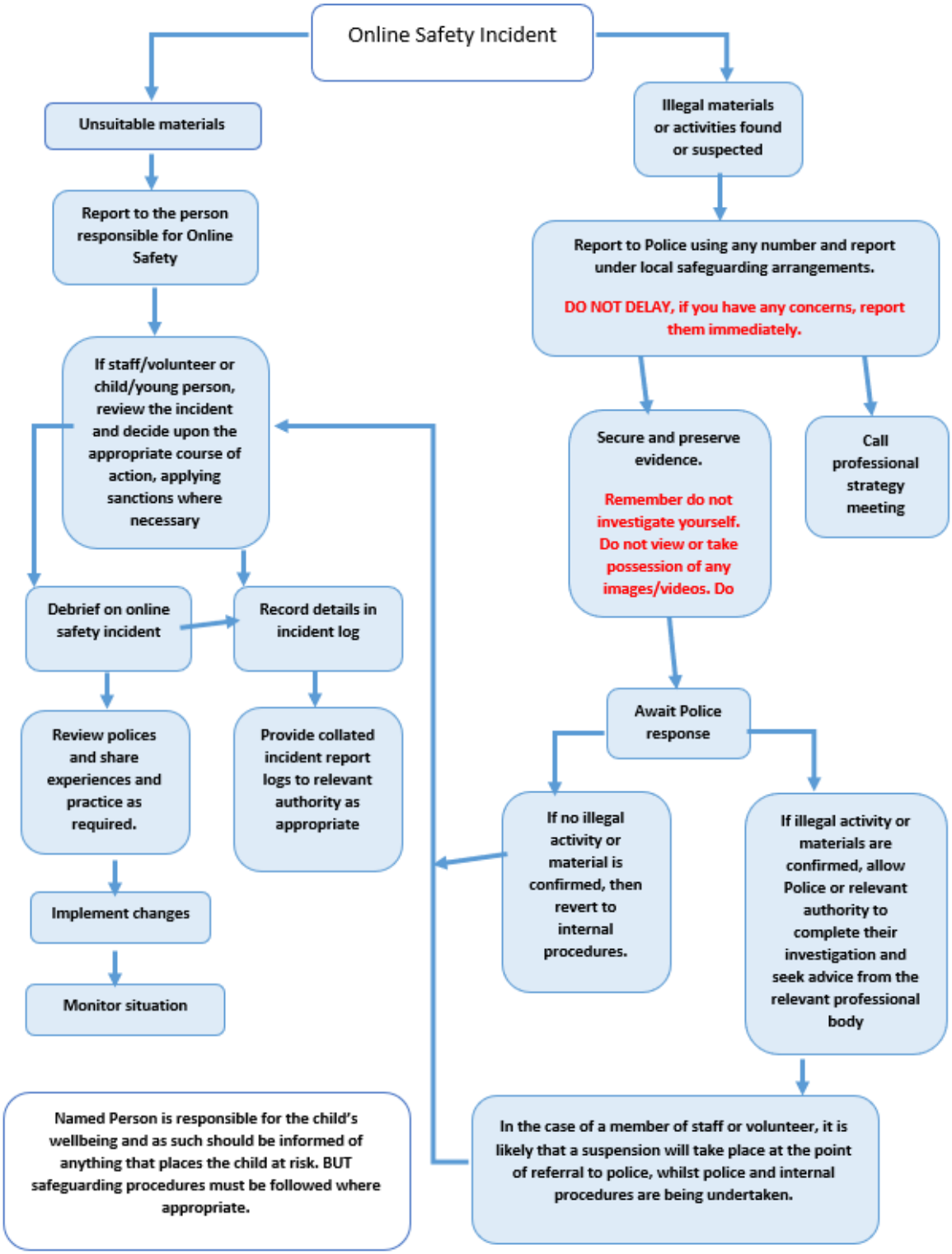
• Using penetration testing equipment (without relevant permission) N.B. Broad Hinton Primary School will decide whether these should be dealt with internally or by the police. Serious or repeat offences should be reported to the police. Under the Cyber-Prevent agenda the National Crime Agency has a remit to prevent young people becoming involved in cyber-crime and harness their activity in positive ways					
Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school/academy				X	
Revealing or publicising confidential or proprietary information (e.g. financial/personal information, databases, computer/network access codes and passwords)				X	
Unfair usage (downloading/uploading large files that hinders others in their use of the internet)				X	
Using school systems to run a private business				X	
Infringing copyright				X	
On-line gaming (educational)		X			
On-line gaming (non-educational)				X	
On-line gambling				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.

Illegal Incidents

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



Other Incidents

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

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

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

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

School actions & sanctions

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

with through normal behaviour/disciplinary procedures as outlined in the disciplinary policy from Wiltshire Council.

Acknowledgements

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

Copyright of these template policies is held by SWGfL. Schools/academies and other educational institutions are permitted free use of the Template Policies for the purposes of policy writing, review and development. Any person or organisation wishing to use the document for other purposes should seek consent from SWGfL (onlinesafety@swgfl.org.uk) and acknowledge its use.

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

© South West Grid for Learning Trust Ltd 2020

Written: February 2022 to be reviewed annually
September 2023
September 2024
April 2026
September 2026