Great Bedwyn C. E. Primary School

Online Safety Policy

Date of Last Review: September 2020
Date to be Reviewed: September 2022
Review Body: Full Governing Body

1. Scope and aims of the Policy

This policy applies to all members of the school community (including staff, pupils, volunteers, parents / carers, visitors, community users) who have access to and are users of school ICT systems, both in and out of the school. This policy also applies to access to the internet and use of information communication devices, including personal devices, or where pupils / staff have been issued with devices off-site.

Great Bedwyn Primary school believes that online internet safety is a fundamental part of safeguarding pupils and adults in the digital world when using internet enabled devices. We recognise that the internet and information communication technologies are an important part of everyday life, therefore, the school community must be supported in learning about online safety and how to develop strategies to manage and respond to risk in the digital world.

The purpose of this policy is to:

- Safeguard and protect all members of the Great Bedwyn Community when online
- Identify key expectations of all members of the school community with regards to the safe and responsible use of technology and internet enabled devices.
- Raise awareness of the benefits and risks of technology.
- Enable staff to work safely and responsibly, role model positive behaviour online and be aware of the need to manage their own standards and practise when using technology.
- Identify clear procedures that are required when responding to online safety concerns.

2. Roles and Responsibilities

Governors:

- Governors are responsible for the approval, implementation, monitoring and review of the Online Safety Policy.

Principal:

- The Principal has a duty of care for ensuring the safety (including online safety) of members of the school community,
- The Principal and the Computing subject leader are aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff.
- The Principal is responsible for ensuring that the Computing subject leader and other relevant staff receive suitable training to enable them to carry out their online safety roles and to train other colleagues, as relevant.

Computing subject leader:

- takes day to day responsibility for online safety issues and has a leading role in establishing and reviewing the school online safety policy.
- 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 'internal' training and advice for staff
- liaises with technical staff from Oakford

School internet and computer support technical staff (Oakford):

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 guidance that may apply
- that users may only access the networks and devices through properly enforced password protection in which passwords are regularly changed
- 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 network / internet / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the Principal / Computing subject leader 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
- they report any suspected misuse or problem to the Principal / Computing subject leader 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 the curriculum and taught regularly throughout the academic year in all year groups through the Online Safety scheme of work.
- pupils understand and follow the Online Safety Policy and acceptable use Agreement
- pupils have a good understanding of research skills and in KS2, 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 planned, pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches

Designated Safeguarding Lead and Deputy 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
- cyber-bullying

Pupils:

- are responsible for using the school digital technology systems in accordance with the Pupil Acceptable Use Agreement
- have a good understanding of research skills and in KS2, 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 personal mobile devices and digital cameras. They should also know and understand policies on the taking / use of images and on cyber-bullying.
- should understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the school's Online Safety Policy covers their actions out of school, if related to their membership of the school.

Parents / Carers:

Parents / Carers play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way. The school will take every opportunity to help parents understand these issues through newsletters, leaflets, and website 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.

3. Internet access

- The school will maintain a current record of all staff and pupils who are granted access to the school's devices and systems.
- All staff, pupils and visitors will sign the Acceptable Use Policy before using any school resources.
- Parents will be informed that pupils will be provided with supervised internet access which is appropriate to their age and ability.
- Parents / carers will be asked to read the Acceptable Use Policy for pupil access and discuss it with their child, where appropriate.

4. The school website

The school will ensure that information posted on the school website meets the requirements as identified by the Department for Education.

The contact details on the school website will be the school setting/address, email and telephone number. Staff personal contact information will not be published. Where the school has parental permission, photographs and the first name of pupils may be published on the school website.

The website will comply with the guidelines for publications including accessibility respect for intellectual property rights, privacy policies and copyright.

The administrator password for the school website will be safeguarded with an appropriately strong password.

The school will post information about Safeguarding, including online safety, on the school website for members of the school community.

5. Publishing images and videos online by the school

- The school will ensure that all images and videos shared online are used in accordance with the school image use policy.

6. Managing email

- All members of staff will be issued with a specific school email address to use for any official communication. This school email address must not be used for personal use.
- Any electronic communication which contains any content which could be subject to data protection legislation will only be sent using a secure encrypted email.
- Members of the school community must immediately report any offensive communication
- Staff will be encouraged to develop an appropriate work life balance when responding to email. Staff should direct all communication with parents through the 'admin@' address and avoid direct communication with parents using their school email accounts.
- School email addresses should be used for official work purposes only.
- School email addresses must not be used for setting up personal social media accounts.

7. Learning Platforms and blogs

The school uses Class Dojo to share learning with Parents

- SLT and staff will regular monitor the use of Class Dojo by families and staff, in particular message and communication tool and publishing facilities.
- Staff and families will be advised about acceptable conduct and use when using an online tool for learning.
- Only members of the current pupil, staff and community will have access to the class account.
- When a user leaves the school their account or rights to relevant content will be disabled.

The school uses TEAMs to share learning with pupils

- SLT will regularly monitor the uses of TEAMs by staff and pupils, in particular live teaching sessions
- Staff and families will be reminded of the acceptable use policy and home School agreement when using an online tool for learning.
- When a user leaves the school their account will be disabled.

8. Education

Pupils:

- Internet use is a key feature of educational access and all children will receive age and ability appropriate education to support and enable them to develop strategies to respond to use the internet effectively.

- Internet safety is taught in all classes as part of Computing lessons.
- The school's internet access will be designed to enhance and extend education.
- Access levels to the internet will be reviewed to reflect the curriculum requirements and the age and ability of pupils.
- All staff members are aware that they cannot rely on filtering alone to safeguard children and supervision, classroom management and education about safe and responsible use is essential.
- Supervision of pupils will be appropriate to their age and ability.
- EYFS and Year 1 pupils will access the internet by adult demonstration and directly supervised access to specific and approved online materials which support the learning outcomes planned for the pupils' age and ability.
- Year 2 - 6 pupils will be supervised when using age appropriate search engines and online tools and activities, being teacher led when necessary; pupils will be directed to online material and resources which support the learning outcomes planned for the pupils' age and ability.
- A planned online safety curriculum is provided as part of Computing and PHSE / and is regularly revisited throughout the year in all year groups.
- Key online safety messages are reinforced as part of a planned scheme of work
- All school owned devices will be used in accordance with the Acceptable Use policy as well as appropriate safety and security measures in place.
- Staff will always evaluate websites, tools and apps fully before use in the classroom or recommending at home.
- Pupils will be educated in the effective use of the internet in research, including the skills of retrieval and evaluation.
- pupils should be taught in 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
- where appropriate, 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 pupils visit. The pupils will also be given research skills to identify suitable websites to use.
- 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 (Oakford) 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 via the Computing Subject Leader.

Parents / Carers:

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

- Letters, newsletters, presentations from external agencies where appropriate
- High profile events / campaigns e.g. Safer Internet Day
- Reference to the relevant web sites / publications through the school website

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:

- Regular 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 annually.
- All new staff should receive online safety training as part of their induction programme, ensuring that they fully understand the school Online Safety Policy and Acceptable Use Agreements.
- The Computing subject leader will receive regular updates through attendance at external training events (eg from SWGfL / LA / other relevant organisations) and by reviewing guidance documents released by relevant organisations.
- This Online Safety Policy and its updates will be presented to and discussed by staff in staff meetings / INSET days.
- The Computing subject leader will provide advice / guidance / training to individuals as required.

Governors:

- The LGB should take part in online safety training / awareness sessions, where appropriate.
- The LGBr should attend training provided by the Local Authority / National Governors Association / or other relevant organisation (e.g. SWGfL) for Governors with responsibility for online safety.
- The LGB should participate in school information sessions for staff or parents / carers when appropriate.

9. Technical – infrastructure / equipment, filtering and monitoring

The school technical support team (Oakford) will be responsible for ensuring that the school infrastructure / network is as safe and secure as is reasonably possible. The school will ensure that policies and procedures approved within this policy are implemented. The school 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, by Oakford, 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 Oakford
- Servers, wireless systems and cabling must be securely located and physical access restricted by Oakford
- All users will have clearly defined access rights to school technical systems and devices.

- All users at KS1, KS2 and EYFS will have a class log on, however, upper KS2 will be provided with a username and secure password by the Computing subject leader who will keep an up to date record of users and their usernames.
- All users are responsible for the security of their username and password and will be required to change their password regularly.
- The “administrator” passwords for the school ICT system, used by Oakford must also be available to the Principal and Computing subject leader.
- The Computing subject leader is responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations
- Internet access is filtered for all users. Illegal content (child sexual abuse images) is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list (Provided by Oakford). 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 should ensure that children are safe from terrorist and extremist material when accessing the internet.
- The school has provided enhanced / differentiated user-level filtering
- Oakford 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 by Oakford. The school infrastructure and individual workstations are protected by up to date virus software, installed, monitored and maintained by Oakford.
- Staff and Volunteer / Visitor Acceptable Use Policy is in place for the provision of temporary access of “guests” (eg trainee teachers, supply teachers, visitors) onto the school systems.
- An agreed policy is in place regarding the extent of personal use that users (staff / pupils / community users) are allowed on school devices that may be used out of school is outlined in the Staff / Volunteers / Visitors Acceptable Use Policy.
- The use of removable media (eg memory sticks / CDs / DVDs) by users on school devices must be encrypted or otherwise secured.

10. Mobile Technologies (including BYOD/BYOT)

Mobile technologies including mobile phones, tablets, laptops, MP3 players and other similar devices are rapidly becoming part of daily life for all of the school community. It is important that all members of the school community adhere to the Acceptable Use Policy and guidance outlined in the Online safety policy.

Expectations for safe use of personal devices and mobile phones

- All use of personal devices and mobile phones will take place in accordance with the Acceptable Use Policy.
- Personal electronic devices brought on site by the user are the user’s responsibility at all times. The school accepts no responsibility for the loss, damage or theft of such items.

- Mobile phones and personal devices are not permitted to be used in front of the children. Parents / Carers should endeavor to only take pictures of their own child during events such as performances and sports day and must not upload any images of children other than their own without parental permission of the pupils included in the image.
- When on trips, including residentials, contact with parents / carers should be conducted through the school or school mobile phone. Staff personal mobiles will only be used in exceptional circumstances.
- All staff members are advised to ensure that their personal electronic devices, including mobile phones, should not contain any content which may be considered offensive, derogatory or would otherwise contravene school policy.

Pupils use of personal devices and mobile phones

- Pupils will be educated regarding the safe and appropriate use of personal devices and mobile phones
- Pupils should not bring any personal devices or mobile phones onto the school premises.
- Should a pupil need to bring a personal device or mobile phone into school, it should be handed in to the school office (where it will be safely stored) and collect it at the end of the school day.

Staff use of personal devices and mobile phones

- Members of staff are not permitted to use their own personal mobile phones or devices to contact pupils and their families within or outside of the setting in a professional capacity unless in exceptional circumstances.
- Staff will not use personal devices or mobile phones to take pictures or videos of pupils and will only use work-provided equipment for this purpose.
- Staff will not use any personal devices directly with the children and will only use work-provided equipment during lessons and educational activities.
- Staff personal mobile phones will be switched off/switched to silent during lesson times and must not be used in pupil areas during the school day. They should be stored safely and away from pupils.

Visitors use of personal devices and mobile phones

- Parents/carers must use mobile phones and personal devices in accordance with the acceptable use policy.
- Use of personal devices and mobile phones is not permitted in pupil areas during the school day.
- Use of mobile phones and personal devices by visitors and parents / carers to take photos or images must take place in accordance with the school image use policy.
- Staff will be expected to challenge concerns when safe and appropriate and will always inform the Designated Safeguarding Lead of any breaches of use by visitors.

11. Use of digital and video images

- 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 pupils are published on the school website / 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 in the digital / video images, without obtaining permission from the parents / carers of pupils involved.

- Staff and volunteers are allowed to take digital / video images to support educational aims, but must follow school images policy. Those images should only be taken on school equipment, the personal equipment of staff should not be used for such purposes.
- Care should be taken when taking digital / video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- pupils must not take, use, share, publish or distribute images of others without their permission
- Photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with good practice guidance on the use of such images.
- Pupils' full names will not be used anywhere on a website, particularly in association with photographs.
- Pupil's work can only be published with the permission of the pupil and parents or carers.

12. Data Protection

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 which states that personal data must be:

- Fairly and lawfully processed
- Processed for limited purposes
- Adequate, relevant and not excessive
- Accurate
- Kept no longer than is necessary
- Processed in accordance with the data subject's rights
- Secure
- Only transferred to others with adequate protection.

12.1 Management of applications (apps) used to record children's progress (2Simple in EYFS and Tapestry)

* Only school issued devices will be used for apps that record and store children's personal details, attainment or photographs. Personal staff mobile phones or devices will not be used to access or upload content to any apps which record and store children's personal details, attainment or images.

* Devices will be appropriately encrypted if taken off site to prevent a data security breach in the event of loss or theft (iPads and the App are pin protected).

13. Social Media - Protecting Professional Identity

All adults who work or volunteer in school, are expected to adhere to all relevant poicies.

14. Responding to Online incidents and safeguarding concerns

- All members of the school community will be made aware of the range of online risks that are likely to be encountered including sexting, online/cyber bullying etc. This will be highlighted within staff training and educational approaches for pupils.

- All members of the school community will be informed about the procedure for reporting online safety (e-Safety) concerns, such as breaches of filtering, sexting, cyberbullying, illegal content etc (covered within CP training for all staff).
- The Designated Safeguarding Lead (DSL) will be informed of any online safety (e-Safety) incidents involving child protection concerns, which will then be recorded.
- The DSL will ensure that online safety concerns are escalated and reported to relevant agencies in line with the Wiltshire Safeguarding Children Board thresholds and procedures.
- Complaints about online/cyber bullying will be dealt with under the School's anti-bullying policy and procedure.
- Any complaint about staff misuse will be referred to the Principal.
- Staff will be informed of the whistleblowing procedure.
- All members of the school community will need to be aware of the importance of confidentiality and the need to follow the official school procedures for reporting concerns.
- All members of the school community will be reminded about safe and appropriate behaviour online and the importance of not posting any content, comments, images or videos online which cause harm, distress or offence to any other members of the school community.
- The school will manage online safety (e-Safety) incidents in accordance with the school behaviour policy where appropriate.
- The school will inform parents/carers of any incidents of concerns as and when required.
- If the school is unsure how to proceed with any incidents of concern, then the incident will be escalated to the Wiltshire Safeguarding Team.
- Parents and children will need to work in partnership with the school to resolve issues.

15 Procedures for Responding to Specific Online Incidents or Concerns

Responding to concerns regarding Youth Produced Sexual Imagery or "Sexting"

- The school will ensure that staff and age appropriate pupils are made aware of the potential social, psychological and criminal consequences of sharing, possessing and creating youth produced sexual imagery (known as "sexting").
- The school views "sexting" as a safeguarding issue and all concerns will be reported to and dealt with by the Designated Safeguarding Lead.

Responding to concerns regarding Online Child Sexual Abuse and Exploitation

- The school will ensure that staff are made aware of online child sexual abuse, including exploitation and grooming including the consequences, possible approaches which may be employed by offenders to target children and how to respond to concerns.
- The school views online child sexual abuse as a safeguarding issue and all concerns will be reported to and dealt with by the Designated Safeguarding Lead.
- If pupils at other schools are believed to have been targeted then the school will seek support from the Wiltshire Safeguarding Team to enable other schools to take appropriate action to safeguarding their community.

Responding to concerns regarding Indecent Images of Children (IIOC)

- The school will ensure that all members of the community are made aware of the criminal nature of Indecent Images of Children (IIOC) including the possible consequences.
- If the school are made aware of an incident of IIOC, then the school will:

    - Ensure that the Designated Safeguard Lead is informed or another member of staff in accordance with the school whistleblowing procedure.
    - Contact the police regarding the images and quarantine any devices involved until police advice has been sought.
    - Inform the Local Authority Designated Officer (LADO) and other relevant organisations in accordance with the schools managing allegations policy.
    - Follow the appropriate school policies regarding conduct.

Responding to concerns regarding radicalisation and extremism online

- The school will take all reasonable precautions to ensure that pupils are safe from terrorist and extremist material when accessing the internet in schools and that suitable filtering is in place which takes into account the needs of pupils.
- When concerns are noted by staff that a pupil may be at risk of radicalisation online then the Designated Safeguarding Lead (DSL) will be informed immediately and action will be taken in line with the safeguarding policy.
- Online hate content directed towards or posted by specific members of the community will be responded to in line with existing school policies, including anti-bullying, behaviour etc. If the school is unclear if a criminal offence has been committed then the Designated Safeguarding Lead will obtain advice immediately via the Wiltshire Safeguarding Team and/or Wiltshire Police.
- All staff will have taken part in PREVENT training.

Responding to concerns regarding cyberbullying

- Cyberbullying, along with all other forms of bullying, of any member of the Great Bedwyn Community will not be tolerated. Full details are set out in the school policies regarding anti-bullying and behaviour.
- All incidents of online bullying reported will be recorded.
- There are clear procedures in place to investigate incidents or allegations and support anyone in the school community affected by online bullying.
- If the school is unclear if a criminal offence has been committed then the Designated Safeguarding Lead will obtain advice immediately through the Education Safeguarding Team and/or Wiltshire Police.
- Pupils, staff and parents/carers will be advised to keep a record of cyberbullying as evidence.
- Pupils, staff and parents/carers will be required to work with the school to support the approach to cyberbullying and the schools e-Safety ethos.

16. 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:

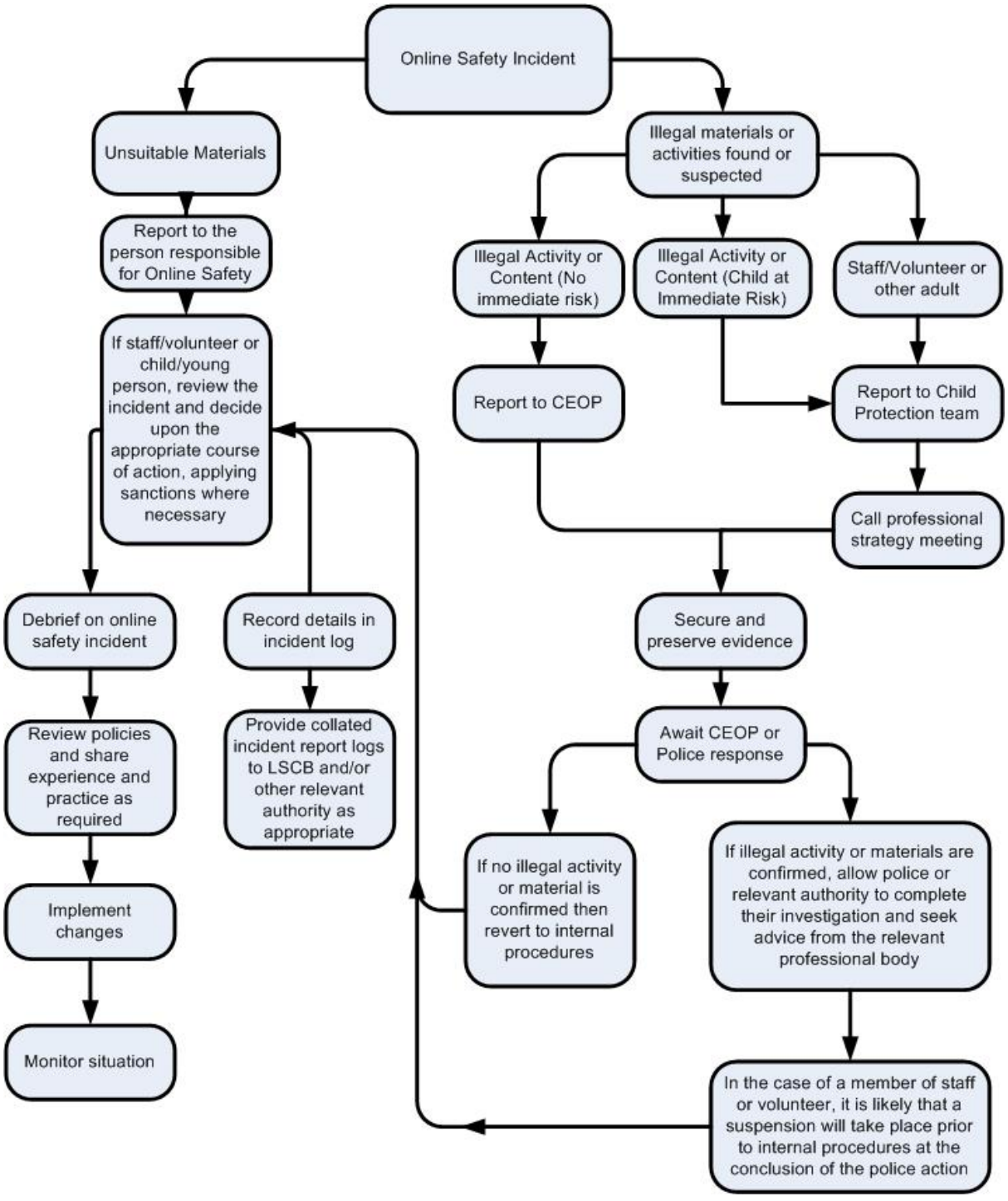
User Actions	Acceptable	Acceptable at certain times	Acceptable for named uusers	Unacceptable	Unacceptable and illegal

Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	Child sexual abuse images –The making, production or distribution of indecent images of children. Contrary to The Protection of Children Act 1978					X
	Grooming, incitement, arrangement or facilitation of sexual acts against children Contrary to the Sexual Offences Act 2003.					X
	Possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character) Contrary to the Criminal Justice and Immigration Act 2008					X
	Criminally racist material in UK – to stir up religious hatred (or hatred on the grounds of sexual orientation) - contrary to the Public Order Act 1986					X
	Pornography				X	
	Promotion of any kind of discrimination				X	
	threatening behaviour, including promotion of physical violence or mental harm				X	
	Promotion of extremism or terrorism				X	
	Any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute				X	
Using school systems to run a private business					X	
Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school / 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 (personal)					X	
Use of social media					X	
Use of messaging apps					X	
Use of video broadcasting e.g. Youtube				X		

17. Responding to incidents of misuse

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) for responding to online safety incidents and report immediately to the police.



Other Incidents

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

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

- Have more than one senior member of staff / volunteer involved in this process. This is vital to protect individuals if accusations are subsequently reported.
- Conduct the procedure using a designated computer that will not be used by young people and if necessary can be taken off site by the police should the need arise. Use the same computer for the duration of the procedure.
- It is important to ensure that the relevant staff should have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
- Record the URL of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed and attached to the form (except in the case of images of child sexual abuse – see below)
- Once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does then appropriate action will be required and could include the following:
    - Internal response or discipline procedures
    - Involvement by Local Authority / 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 the school and possibly the police and demonstrate that visits to these sites were carried out for safeguarding purposes. The completed form should be retained by the group for evidence and reference purposes.