

# **Chapmanslade School**

## **Online Safety Policy**

### **Rationale**

This policy applies to all members of Chapmanslade School (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 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.

### **Aims**

This policy outlines expectations for staff and pupil's online safety, as well as how to deal with issues that may arise online. 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**

#### **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. The designated governor for safeguarding will be informed of online safety incidents and corresponding logs.

#### **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. They will use Online Safety BOOST 'Incident Response Tool' for guidance and support (<https://boost.swgfl.org.uk/>).
- The Headteacher and Senior Teacher 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.

### 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 Local Authority if necessary
- liaises with school technical staff, currently the managed school provider (Soft Egg)
- receives reports of online safety incidents and creates a log of incidents to inform future online safety developments
- reports regularly to Senior Leadership Team

### Technical staff

The school's current managed school provider and Computing Subject Leader will ensure the following:

- 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, 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 Headteacher / Online Safety Lead for investigation / action / sanction
- that monitoring software / systems are implemented and updated

### 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 Headteacher / Online Safety Lead for investigation / action / sanction
- all digital communications with 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 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
- peer-on-peer abuse

#### 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 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 parents' evenings, newsletters, letters, website and information about national / local online safety campaigns / literature. Parents and carers will be encouraged to support the school in promoting good online safety practice and to follow guidelines on the appropriate use of:

- digital and video images taken at school events
- their personal devices in the school

## **Education and Training**

### Pupils

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.

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 is provided as part of Computing / PHSE / other lessons and should be regularly revisited
- Key online safety messages should be reinforced as part of the computing curriculum
- 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
- In line with the Counter Terrorism and Securities Act 2015, 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's Acceptable Use Agreement and encouraged to adopt safe and responsible use both within and outside school.

- Staff should act as good role models to pupils in their use of digital technologies, the internet and mobile devices
- Where pupils are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit.

### Parents / Carers

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

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

- Curriculum activities
- Letters, newsletters, web site
- Parents / Carers evenings / sessions
- High profile events / campaigns e.g. Safer Internet Day
- Reference to the relevant web sites / publications e.g. [swgfl.org.uk](http://swgfl.org.uk)  
[www.saferinternet.org.uk/](http://www.saferinternet.org.uk/) <http://www.childnet.com/parents-and-carers>

### 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:

- An audit of the online safety training needs of all staff will be carried out regularly.
- A planned programme of formal online safety training will be made available to staff. This will be regularly updated and reinforced depending on the results of the above audit.
- All new staff should receive online safety training as part of their induction programme, ensuring that they fully understand the school Online Safety Policy and Acceptable Use Agreements.
- The Online Safety Lead should receive regular updates by reviewing guidance documents released by relevant organisations and through attendance at external training where necessary.
- This Online Safety Policy and its updates will be presented to and discussed by staff in staff / team meetings / INSET days.

- The Online Safety Lead will provide advice / guidance / training to individuals as required.
- In the unlikely event that a teacher needs to research topics (eg racism, drugs, discrimination) that would normally result in internet searches being blocked, they can request that the Technical Staff 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 and will need to be agreed with the headteacher.

### Governors

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

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

### **Technical – infrastructure / equipment, filtering and monitoring**

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.

The school's managed service provider (currently Soft Egg) 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.

- School technical systems will be managed in ways that ensure that the school meets recommended technical requirements
- There will be regular reviews and audits of the safety and security of school technical systems
- Servers, wireless systems and cabling must be securely located and physical access restricted
- All users will have clearly defined access rights to school technical systems and devices.
- All staff users will be provided with a username and secure password by the managed service provider. The School Business Manager 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 on a regular basis.

- Chapmanslade has chosen to use shared class username and passwords for pupils. However, teachers will advise children that this is unique and should not be replicated outside of school.
- The “master / administrator” passwords for the school ICT systems, used by the Network Manager (or other person) must also be available to the Headteacher or School Business Manager and kept in a secure place (eg school safe)
- The School Business Manager is responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations
- Internet access is filtered for all users by SWGfL. 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.
- The school has provided enhanced / differentiated user-level filtering, meaning that pupils and staff can access different materials.
- 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.
- If users need to report any actual / potential technical incident / security breach, they must report to the headteacher or Online Safety Lead.
- 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.
- An agreed policy is in place for the provision of temporary access of “guests” (eg trainee teachers, supply teachers, visitors) onto the school systems. The School Business Manager will provide them with access if deemed necessary.
- The use of personal removable media (eg memory sticks / CDs / DVDs) by users on school devices is not permitted.
- Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured.

### **Mobile Technologies**

Mobile technology devices may be school owned/provided or personally owned and might include: smartphone, tablet, notebook / laptop or other technology that usually has the capability of utilising the school’s wireless network. The device then has access to the wider

internet which may include the school'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 procedures should be consistent with and inter-related to other relevant school policies 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 Agreements for staff, pupils/students and parents / carers will give consideration to the use of mobile technologies

The school allows:

|                        | School Devices               |                                 | Personal Devices |             |               |
|------------------------|------------------------------|---------------------------------|------------------|-------------|---------------|
|                        | School owned for single user | School owned for multiple users | Student owned    | Staff owned | Visitor owned |
| Allowed in school      | Yes                          | Yes                             | No               | Yes         | Yes           |
| Full network access    | Yes                          | Yes                             | N/A              | No          | No            |
| Internet only          | N/A                          | N/A                             | N/A              | No          | No            |
| Limited network access | N/A                          | N/A                             | N/A              | No          | No            |

The school has provided technical solutions for the safe use of mobile technology for school devices:

- All school devices are controlled through the use of Mobile Device Management (MDM) software
- Appropriate access control is applied to all mobile devices according to the requirements of the user (e.g Internet only access, network access allowed, shared folder network access)
- The school has addressed broadband performance and capacity to ensure that core educational and administrative activities are not negatively affected by the increase in the number of connected devices
- For all mobile technologies, filtering will be applied to the internet connection and attempts to bypass this are not permitted
- Appropriate exit processes are implemented for devices no longer used at a school location or by an authorised user.



- All school devices are subject to routine monitoring
- Pro-active monitoring has been implemented to monitor activity

### **Use of digital and video images**

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

- When using digital images, staff should inform and educate 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 by the School Business Manager
- 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 is 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. This will be mentioned to parents before school events.
- 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 must never be used for such purposes.
- Care should be taken when taking digital / video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Pupils must not take, use, share, publish or distribute images of others without their permission
- Photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with good practice guidance on the use of such images.
- Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs.

## **Data Protection**

Personal data will be recorded, processed, transferred and made available according to the current data protection legislation. This is detailed in our Data Protection Policy.

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.
- Use personal data only on secure password protected computers and other devices, ensuring that they are properly “logged-off” at the end of any session in which they are using personal data.
- No sensitive data is to be stored on the computer itself. It should be saved on the designated server and accessed through remote desktop.
- Transfer data using encryption or secure password protected devices.
- The data must be encrypted or password protected.
- The data must be securely deleted from the device, in line with school policy once it has been transferred or its use is complete.
- If emails can be accessed through mobile devices, this should be password or fingerprint protected. No downloads should be made to the device itself.

## **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.
- Pupils are not to bring in mobile phones or other devices such as tablets or smart watches.
- Users must immediately report, to the nominated person – in accordance with the school policy, the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication. (Online Safety BOOST includes an anonymous reporting app Whisper – <https://boost.swgfl.org.uk/>)
- There should be no digital communication between staff and pupils or parents / carers (email, social media, chat, blogs etc) unless it is through the admin officer or has been agreed with the headteacher.
- 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**

For more information, please see our Social Media Policy.

All schools, academies, MATs and local authorities have a duty of care to provide a safe learning environment for pupils and staff. Schools/academies, 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.
- 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
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information

### **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

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

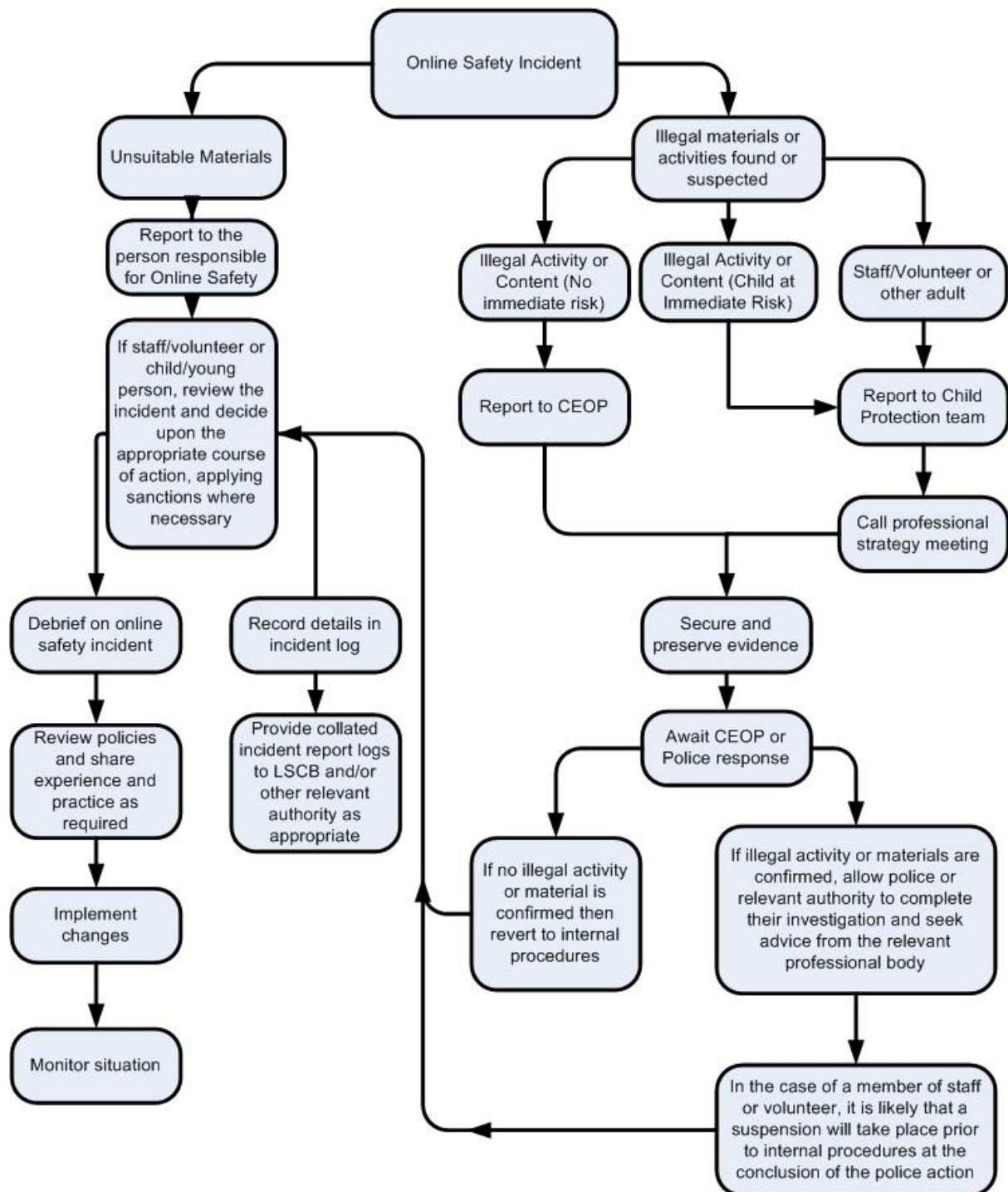
|  |  |   |  |   |  |
|--|--|---|--|---|--|
| Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school                                   |  |   |  | X |  |
| Infringing copyright   |  |   |  | X |  |
| Revealing or publicising confidential or proprietary information (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). E.g Mathletics   |  | X |  |   |  |
| On-line gaming (non-educational)   |  |   |  | X |  |
| On-line gambling   |  |   |  | X |  |
| On-line shopping / commerce (for school purposes)  |  | X |  |   |  |
| File sharing   |  | X |  |   |  |
| Use of social media  |  |   |  | X |  |
| Use of messaging apps (see Acceptable Use and Code of Conduct for more details)  |  | 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 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
  - other criminal conduct, activity or materials
- Isolate the computer in question as best you can. Any change to its state may hinder a later police investigation.

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

## School Actions & 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 follows:

| Students / Pupils Incidents  | Possible Actions / Sanctions |                      |                 |  |                         |   |         |   |
|--|------------------------------|----------------------|-----------------|--|-------------------------|---|---------|---|
|  | Refer to class teacher       | 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               |  |                         |   |         |   |
| 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  | 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 the school network, using another pupil's account  | X                            | X                    |                 | X  | X                       |   |         |   |
| Attempting to access or accessing the school network, using the account of a member of staff   | X                            | X                    |                 | X  | X                       | X   | X       |   |
| Corrupting or destroying the data of other users   | X                            | 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 |   | X |   |
| Continued infringements of the above, following previous warnings or sanctions  |   | X | X |   | X | X |   | X |
| Actions which could bring the school into disrepute or breach the integrity of the ethos of the school                  |   | X |   |   | X | X | X |   |
| Accidentally accessing offensive or pornographic material and failing to report the incident                            | X | X |   | X | X |   | X |   |
| Deliberately accessing or trying to access offensive or pornographic material   | X | X |   | X | X | X | X |   |
| Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act | X | X |   | X | X |   | X |   |

### Possible Actions / Sanctions

#### Staff Incidents

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

## Review

This policy will be published on the school website and shall be reviewed no later than every three years by the Governing Board.

Approved – October 2021

Next Review – October 2024 or sooner if statutory guidance changes

## Acknowledgements

This policy has been developed using the SWGfL model policy for online safety.