Brandwood Community School

Online Safety Policy

Approved by the Teaching & Learning Governor Committee: May 2025
Review Date: May 2026

Introduction

In the modern world, learners are growing up surrounded by online life. This offers many beneficial opportunities but also creates challenges, risks and threats. At Brandwood Community School we aim to equip our learners with the knowledge to be able to use technology to their best advantage in a safe, considered, and respectful way.

Our school community recognises the importance of treating online safety as an ever-present, serious safeguarding issue and consequently view the teaching of online safety as a whole school issue and the responsibility of all staff. It is important to protect and educate both learners and staff and have supportive mechanisms, policies, and protocols in place to support the whole school community.

Legislation set out by numerous Acts of Parliament relate to online safety when considering the safeguarding of both staff and learners in schools and reviewing the school's adherence to these is an integral part of every Ofsted review. The safeguarding aspects of online safety are evident in all our ICT/safeguarding policies and procedures throughout the school, and it is essential that, given the constantly developing area of technology, these are kept under regular review.

Under the General Data Protection Regulation (GDPR), the school is responsible for exacting standards of safety and security for personal data that may be processed.

This policy links to all the ICT, safeguarding and other related policies and procedures to reflect how the school deals with online safety issues. The documents referred to in this online safety policy have been developed by various groups including:

- ◊ Governors, including the link governor for online safety
- ◊ Head Teacher, Senior Leadership Team (SLT) and Designated Safeguarding Lead (DSL)
- ◊ Online safety co-ordinator and ICT technical support staff
- ◊ Teachers and support staff
- ◊ Learners
- ◊ Parents and carers

Aims

This policy aims to ensure the use of electronic communication at Brandwood Community School is as safe as possible. This policy applies to all members of the school community (including staff, learners, volunteers, parents and carers, visitors, community users) who have access to, and are users of, school ICT systems, both in and out of school.

We aim to:

- ◊ Ensure the safety and wellbeing of learners is paramount when adults or learners are using the internet, social media or mobile devices
- ◊ Provide staff and volunteers with the overarching principles that guide our approach to online safety
- ◊ Ensure that, as an organisation, we operate in line with our values and within the law in terms of how we use online devices

Roles & Responsibilities

Governors

The governors are responsible for:

- ◊ Ensuring filtering and monitoring systems are in place on the school's ICT resources
- ◊ Ensuring compliance with the Data Protection Act and the GDPR for all personal data held
- ◊ Ensuring that learners are taught about online safety, for example through Personal, Social, Health and Economic (PSHE) Education and through Relationships Education
- ◊ Approving of the online safety policy, for reviewing the effectiveness of the policy and for dealing with issues when they arise
- ◊ Keeping online safety practice and policy in the school under regular review
- ◊ Appointing a nominated link governor for online safety
- ◊ Attending training and awareness sessions as part of their cycle of meetings

Head Teacher & SLT

The Head Teacher is responsible for:

- ◊ Ensuring the online safety of all members of the school community and managing the education of learners and training of staff in online safety and awareness of potential radicalisation in learners through online networks
- ◊ Taking appropriate action if it is felt that any learner of the school may be becoming radicalised
- ◊ Ensuring compliance with the Data Protection Act and GDPR for the processing of personal data
- ◊ Ensuring members of the senior leadership team are aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff, including the Head Teacher
- ◊ Regulating the behaviour of learners when they are off the school site and empowering members of staff to impose disciplinary penalties for inappropriate behaviour in line with the behaviour policy; this is pertinent to incidents of cyber-bullying, or other online safety incidents covered by this policy wherever they are linked to members of the school, even though they may take place out of school

Computing Leads & Subject Lead Link

The Computing Leads & Subject Lead Link are responsible for:

- ◊ Taking day-to-day responsibility for online safety issues and having a leading role in establishing and reviewing the school online safety policy and other related policies, including the safe processing of personal data
- ◊ Ensuring that all members of staff are aware of the procedures that need to be followed in the event of an online safety incident taking place
- ◊ Providing training and advice for staff to ensure that all online safety teaching is carried out in an age-appropriate way
- ◊ Liaising with school ICT technical staff
- ◊ Reporting regularly to the senior leadership team or Head Teacher
- ◊ Receiving training at regular update sessions and by reviewing national and local guidance documents
- ◊ Liaising with the local authority (LA) and reporting to the Head Teacher any suspicions of learners who may be becoming radicalised

Schools ICT

Schools ICT are responsible for ensuring:

- ◊ They follow the DFE digital and technology standards in schools
- ◊ Internet access is filtered for all users. Illegal content is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation Child Abuse Image Content list (CAIC)
- ◊ They provide and maintain filtering and monitoring solutions in line with recommended standards
- ◊ They provide a platform where school should report any content accessible in school but deemed inappropriate
- ◊ There is a clear process in place to deal with requests for filtering changes
- ◊ They provide a solution which enables DSLs and nominated staff to receive alerts by having access to a specific safeguarding email
- ◊ The school's ICT infrastructure is secure and is not open to misuse or malicious attack
- ◊ The school meets the online safety technical requirements outlined in the relevant national and local ICT security policy and/or acceptable use, online safety policy, and guidance
- ◊ Users may only access the school's networks through a properly enforced password protection policy
- ◊ The Head Teacher is informed of any breaches in the processing of personal data
- ◊ They attend appropriate training on a regular basis from approved trainers to support the online safety of all members of the school community
- ◊ The Head Teacher is informed of any suspicions of learners who may be becoming radicalised

Teachers & Support Staff

All staff receive online safety training and understand their responsibilities, as outlined in this policy. An audit of the online safety training needs of all staff is carried out regularly and a record kept on the staff training record by the School Business Manager. Training will be offered as a planned programme of formal online safety training available to all staff. All new staff will receive online safety training as part of their induction programme, ensuring that they fully understand the school online safety policy and acceptable use policies.

Teaching and support staff are responsible for ensuring:

- ◊ They have an up-to-date awareness of online safety matters and of the current school online safety policy
- ◊ They have read, understood, and signed the relevant staff acceptable computer use agreement and staff laptop use agreement, as well as other related policies e.g., staff e-mail, social media, use of personally owned ICT devices and professional identity protection
- ◊ They report any suspected misuse or problem to the Head Teacher, a member of SLT, Computing Lead or class teacher, as appropriate, for investigation, action, or sanction
- ◊ They report any suspected breach of processing personal data to the Head Teacher
- ◊ Digital communications with parents and carers (email/telephone, text messages) are on a professional level and only carried out using official school systems
- ◊ Learners understand and follow the school online safety policy and the acceptable computer use policy
- ◊ Learners have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- ◊ They monitor ICT activity in lessons and in extracurricular and extended school activities
- ◊ They are aware of online safety issues related to the use of mobile phones, cameras and hand-held devices and that they monitor their use and implement current school policies with regards to these devices
- ◊ They are aware of the online safety issues pertaining to email and social media use
- ◊ They are alert to, and report to the Head Teacher, any suspicions of learners who may be becoming radicalised
- ◊ In lessons where internet use is pre-planned, learners are guided to sites checked as suitable for their use and processes are in place for dealing with any unsuitable material that is found in internet searches

Designated Safeguarding Lead (DSL)

The DSL is trained in online safety issues and will be aware of the potential for serious child protection issues to arise from:

- ◊ Sharing of personal data
- ◊ Access to illegal, inappropriate materials
- ◊ Inappropriate online contact with adults or strangers
- ◊ Potential or actual incidents of grooming
- ◊ Cyber-bullying
- ◊ Sexting
- ◊ Suspicions of radicalisation

Learners

Learners are expected to know and understand:

- ◊ Their responsibility for using the school ICT systems in accordance with the acceptable computer use policy and iPad agreements which they will be expected to sign before being given access to school systems
- ◊ The importance of reporting abuse, misuse or access to inappropriate materials, including suspicions of learners who may be becoming radicalised, and know how to report such abuse
- ◊ How to use effective research skills and the need to avoid plagiarism and uphold copyright regulations
- ◊ School policies on the use of mobile phones, digital cameras and hand-held devices, including the school's policy on confiscation of inappropriate items where it relates to the use of mobile phones
- ◊ School policies on the taking or use of images and on cyber-bullying
- ◊ The dangers of social networking sites as well as their benefits
- ◊ The importance of adopting good online safety practice when using digital technologies both in and out of school and realise that the school's online safety policy covers their actions out of school

Parents & Carers

Parents and carers play a crucial role in ensuring that their children understand the need to use the internet and mobile devices in an appropriate way.

Parents and carers will be responsible for:

- ◊ Having regular conversations about staying safe online and encourage their children to speak to them if they come across something worrying online
- ◊ Speaking to their children particularly about the importance of creating a safe online environment, including keeping any log-in details and passwords safe

Resources which support parents and carers to talk to their children about a range of online safety issues, set up home filtering in a child-friendly way, and set up age-appropriate parental controls on digital devices are regularly shared with parents and carers and they are are invited to an online safety meeting every year for further guidance and support.

Research shows that many parents and carers do not fully understand the issues and are less experienced in the use of ICT than their children. The school will therefore take every opportunity to help parents and carers understand these issues through:

- ◊ Sending information on internet safety and the importance of monitoring internet use at home to all parents and carers annually
- ◊ Parents and carers' evenings
- ◊ Newsletters
- ◊ Letters
- ◊ Website information
- ◊ Information about all relevant national and local online safety campaigns and literature
- ◊ Information about useful organisations and support services for reporting online safety issues
- ◊ Sharing the National Online Safety guidance ('Wake up Wednesdays')
- ◊ Parent & Carer Online safety meetings

Visitors entering our school

It is important for the school to inform visitors of all relevant policies regarding their visit and interaction with learners. This ensures a safe and secure environment for everyone.

All visitors must be made aware of the school's policies that relate to their visit and any interactions they may have with pupils. This includes safeguarding, behaviour and confidentiality policies.

Visitors who require access to the Guest WiFi network should be informed that the content accessed on their personal devices is monitored by the school's IT systems. This monitoring is in place to ensure the safety and security of the network and its users.

Online Safety Curriculum

Online safety is taught in specific areas of the curriculum but is also emphasised whenever learners are using computers or devices online. Staff always consider age-appropriateness when speaking of online safety and will be aware of those learners

who may be particularly vulnerable, e.g. looked-after children or those with special needs. The school may use external resources and external visitors to assist in lessons, but appropriate members of staff will check in advance to ensure that they will enhance lessons and that materials used are appropriate for them.

Learners are taught about online safety explicitly in the following curriculum areas:

Relationships Education

- ◊ Online safety and harm
- ◊ Positive, healthy and respectful relationships online
- ◊ The potential positive and negative effects of their online actions
- ◊ How to recognise and show respectful behaviour online
- ◊ Computing in the curriculum
- ◊ Principles of online safety
- ◊ Where to obtain help and support if they are concerned about any online content or contact

Citizenship Curriculum

- ◊ Media literacy online
- ◊ Distinguishing fact from fiction online
- ◊ Online safety throughout the curriculum

Key online safety messages will be reinforced as part of a planned programme of assemblies and tutorial or pastoral activities, including:

- ◊ How to evaluate what they see online ~ to be critically aware of the materials and content they access online and be guided to validate the accuracy of information
- ◊ How to recognise persuasion techniques
- ◊ How to recognise acceptable and unacceptable online behaviour ~ to understand the need for the acceptable use agreement and iPad contracts to adopt safe and responsible use of ICT, the internet and mobile devices both within and outside school
- ◊ How to identify online risks
- ◊ How and when to seek support
- ◊ The need to acknowledge the source of any information used and to respect copyright when using material accessed on the internet

In lessons where internet use is pre-planned, learners are guided to sites checked as suitable for their use and processes are in place for dealing with any unsuitable material that is found in internet searches.

Where learners are allowed to search the internet freely, e.g. using search engines, staff are vigilant in monitoring the content of the websites the learners visit and learners are encouraged to take appropriate safety precautions e.g. using a safe search engine.

Infrastructure Management

The school will be responsible for ensuring that the school infrastructure and network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. The school will also ensure that the relevant people named in the above sections will be effective in carrying out their online safety responsibilities:

- ◊ School ICT systems will be managed in ways that ensure that the school meets the online safety technical requirements outlined in the acceptable use policy and any relevant LA online safety policy and guidance
- ◊ Personal data is held and processed in compliance with the Data Protection Act and GDPR. Personal data must not be sent over the internet or taken off the school site unless safely encrypted or otherwise secured
- ◊ There will be regular reviews and audits of the safety and security of school ICT systems
- ◊ Servers, wireless systems and cabling will be securely located and physical access restricted
- ◊ All users will have clearly defined access rights to school ICT systems. Details of the access rights available to groups of users will be recorded by the network manager and will be reviewed, at least annually
- ◊ All users will be provided with a username and password by the School Business Manager
- ◊ Users are made responsible for the security of their username and password, must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security
- ◊ The school maintains and supports the managed filtering service provided by Bolton Schools ICT. Any filtering issues should be reported immediately to the network manager
- ◊ School ICT technical staff regularly monitor and record the activity of users on the school ICT systems and users are made aware of this in the acceptable use policy
- ◊ The senior leadership team monitor appropriate internet use using FastVue and complete a thorough investigation of any inappropriate search content, taking any appropriate action as a result
- ◊ Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, workstations, handheld devices etc from accidental or malicious attempts which might threaten the security of the school systems and data

- ◊ An agreed policy is in place in the acceptable computer use policy regarding the downloading of executable files by users
- ◊ Agreements are signed by members of staff in possession of school-provided laptops regarding the extent of personal use that users (staff, learners, community users) and their family members are allowed on laptops and other personally owned devices that may be used out of school
- ◊ The school infrastructure and individual workstations are protected by up-to-date virus software

Protocols on Using Digital & Video Images

- ◊ When using digital images, staff inform and educate learners about the risks associated with taking, using, sharing, publishing, and distributing images. They recognise the risks attached to publishing their own images on the internet e.g. on social networking sites
- ◊ If any incidents become known about 'sexting' i.e. the sharing of sexual images of pupils under 18, the DSL should be advised in the first instance
- ◊ Staff 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
- ◊ Any images should only be taken on school equipment. Personal equipment of staff should *not* be used for such purposes
- ◊ 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. Written permission from parents or carers will be obtained

Protocols on Data Protection

Personal data will be recorded, processed, transferred, and made available according to the Data Protection Act and in compliance with the General Data Protection Regulation (GDPR) which state 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

Staff will ensure that they comply with the internal data security policy by:

- ◊ Always taking care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse
- ◊ Using personal data only on secure password protected computers and other devices, and ensuring that they are properly 'logged-off' at the end of any session in which they are using personal data
- ◊ Transferring data using encryption and secure password protected devices

Protocols for Handling Electronic Communications

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 need to be aware that email communications may be monitored
- ◊ Users will be expected to know and understand school policies on email, social media (and other relevant electronic devices protocols.)
- ◊ Users must immediately report, to the nominated person, in accordance with the school policy, the receipt of any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature. Users must not respond to any such email but must follow the procedures in the email policy
- ◊ Any digital communication between staff and learners, parents, or carers (email, chat, VLE etc) must be professional in tone and content

Unsuitable & Inappropriate Activities

Certain activities are referred to in the acceptable use agreements as being inappropriate in a school context and users must not engage in these activities in school or outside school when using school equipment or systems. The school policies on child protection, safeguarding and online safety *must be* followed if any apparent, suspected, or actual misuse involves illegal or inappropriate activity e.g.:

- ◊ Child sexual abuse images
- ◊ Adult material which potentially breaches the Obscene Publications Act
- ◊ Criminally racist material
- ◊ Other criminal conduct, activity, or materials
- ◊ Potential radicalisation of learners

Should any serious online safety incidents take place, the appropriate external authorities will be informed e.g. LADO, police etc. or, for personal data breaches, the Information Commissioner's Office (ICO).

Filtering & Monitoring Systems

The Keeping Children Safe in Education guidance emphasises the critical role that filtering and monitoring play in ensuring online safety within schools. The document stresses that schools must have strong systems in place to manage the use of technology and all staff members must understand their responsibilities regarding online safety. This includes having clear policies for filtering and monitoring both school devices and networks to protect learners from harmful or inappropriate content.

Schools are expected to ensure appropriate filtering and monitoring mechanisms are in place on devices and networks that learners use. This helps prevent access to harmful material and allows schools to monitor activity to protect learners from risks like cyberbullying, exposure to inappropriate content and online predators.

The following procedures are in place to adhere to the KCSIE guidance:

- ◊ Adoption of the filtering and monitoring systems from BoltonICT
- ◊ Use of Lightspeed to monitoring online incidents
- ◊ Updated firewalls through 'Watchguard' which monitor what content is being accessed and blocks any inappropriate websites
- ◊ Robost procedures to deal with any online safety incidents
- ◊ All staff complete annual online safety training, which includes filtering and monitoring
- ◊ Annual online safety audit completed by the DSL
- ◊ Annual online safety risk assessment
- ◊ Development of Apple Classroom

Apple classroom is another level of security within our filtering and monitoring systems. This software allows staff members to monitor live useage from learners' Ipads. Staff are able to view what each child is accessing from their own teacher Ipad to ensure they are only accessing the directed sites and apps. Apple Classroom also enables teachers to freeze learners Ipads on certain apps or sites so they can't access anything else other than what the teacher has directed. This will enable teachers to have a closer oversight of what their learners are using the Ipads for and reduce any inappropriate useage.

The DSL will ensure that the school's safeguarding & child protection policies adequately reflect its approach to online safety, including appropriate filtering and monitoring on school devices and school networks.

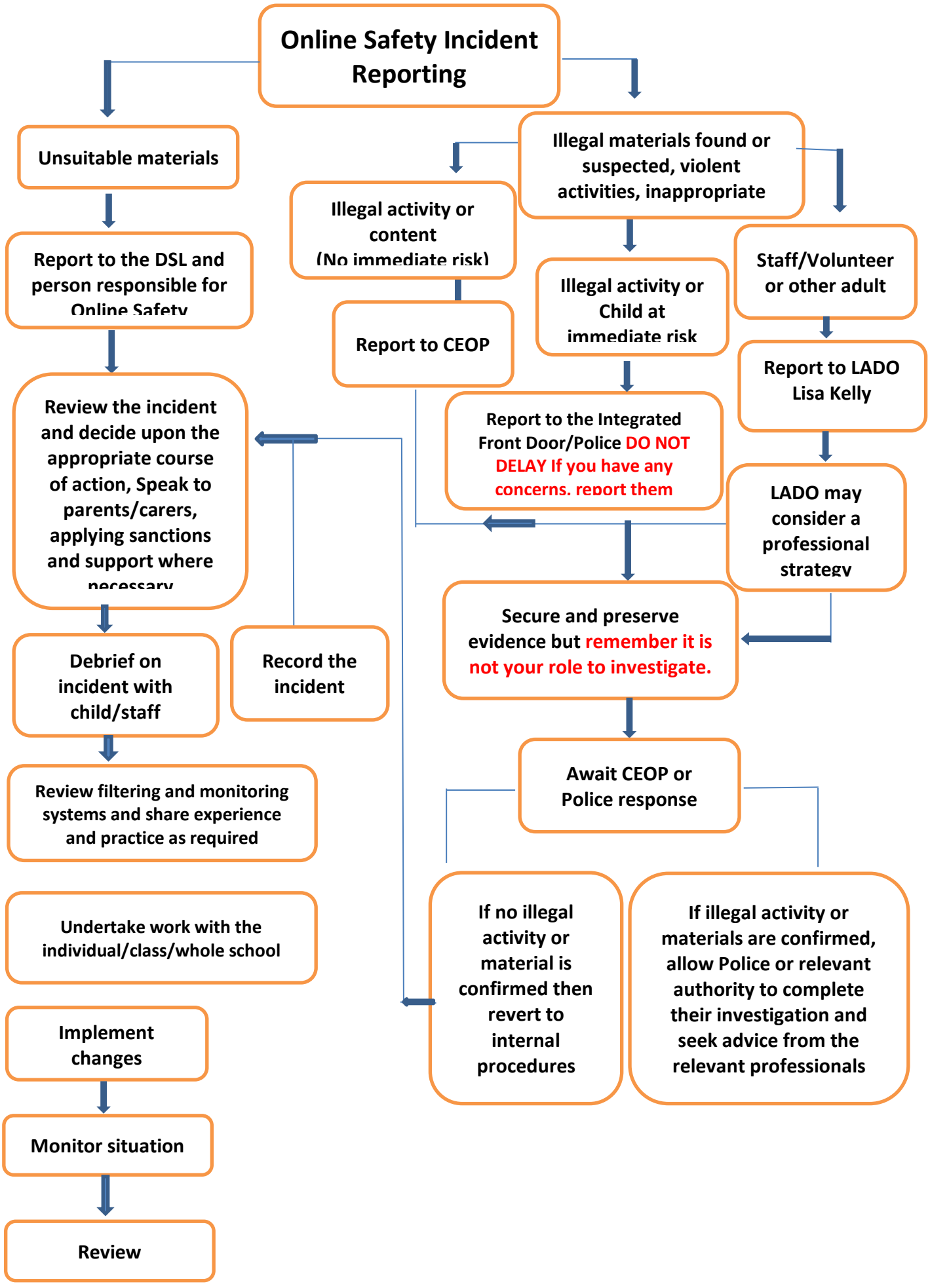
The DSL is responsible for taking any necessary action as per the Online Safety Incident reporting flowchart (Appendix1). This is displayed around the school and in classrooms.

They will arrange regular training and provide annual updates for all staff members about their responsibilities regarding online safety, filtering and monitoring.

Conclusion

If any parent, governor, member of staff or learner requires any further information or advice regarding any aspect of this document please seek out a member of the Senior Leadership Team or contact the school office. This guidance has been compiled in consultation with key staff and the Pupil Inclusion and Community Governor Committee.

Approved by the Teaching & Learning Governor Committee: May 2025
Review Date: May 2026


Online Safety Incident Reporting
Unsuitable materials
Report to the DSL and person responsible for Online Safety
Review the incident and decide upon the appropriate course of action, Speak to parents/carers, applying sanctions and support where necessary
Debrief on incident with child/staff
Record the incident
Review filtering and monitoring systems and share experience and practice as required
Undertake work with the individual/class/whole school
Implement changes
Monitor situation
Review
Illegal materials found or suspected, violent activities, inappropriate
Illegal activity or content (No immediate risk)
Report to CEOP
Illegal activity or Child at immediate risk
Report to the Integrated Front Door/Police DO NOT DELAY If you have any concerns, report them
Staff/Volunteer or other adult
Report to LADO Lisa Kelly
LADO may consider a professional strategy
Secure and preserve evidence but remember it is not your role to investigate.
Await CEOP or Police response
If no illegal activity or material is confirmed then revert to internal procedures
If illegal activity or materials are confirmed, allow Police or relevant authority to complete their investigation and seek advice from the relevant professionals