Somerford Primary School

Online Safety Policy

Updated: May 2025
Review Due: May 2026

Development/Monitoring/Review of this Policy
This online safety policy has been developed by a working group made up of:

- Headteacher
- Online Safety Lead
- Staff
- Governors
- DSL and Deputy DSL's

Schedule for Development/Monitoring/Review

This online safety policy was approved by the Governing Body:	May 2025
The implementation of this online safety policy will be monitored by the:	Online Safety Leader and the Headteacher
Monitoring will take place at regular intervals:	At least once per school year
Governing Body/Governors Sub Committee will receive a report on the implementation of the online safety policy generated by the Online Safety Lead (which will include anonymous details of online safety incidents) at regular intervals:	At least once per school year
The online safety policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to online safety or incidents that have taken place. The next anticipated review date will be:	May 2025
Should serious online safety incidents take place, the following relevant external persons/agencies should be informed:	LA Safeguarding Officer, LADO, Police

The school will monitor the impact of the policy using:

- Logs of reported incidents on My Concern
- Monitoring logs via Content Keeper of internet activity (including sites visited)/filtering – Trailblaze regularly check search histories.
- Trailblaze will monitor network traffic in and around school, including school devices used by staff off site, anything that gets flagged as unusual will be investigated and resolved by DSL's or Online safety lead.

Scope of the Policy

This policy applies to all members of the Somerford Primary School community (including staff, pupils, volunteers, parents/carers, visitors,) 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. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data in the case of both acts, action can only be taken over issues covered by the published Behaviour Policy. The school will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents/carers of incidents of inappropriate online safety behaviour that take place out of school.

Roles and Responsibilities

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

Headteacher and senior leaders

- The headteacher has a duty of care for ensuring the safety (including online safety) of members of the school community and fostering a culture of safeguarding, though the day-to-day responsibility for online safety is held by the Designated Safeguarding Lead, as defined in Keeping Children Safe in Education.
- 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[1].
- The headteacher/senior leaders are responsible for ensuring that the Designated Safeguarding Lead / Online Safety Lead, IT provider/technical staff, and other relevant staff carry out their responsibilities effectively and receive suitable training to enable them to carry out their roles and train other colleagues, as relevant.
- The headteacher/senior leaders will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal online safety monitoring role.
- The headteacher/senior leaders will receive regular monitoring reports from the Designated Safeguarding Lead / Online Safety Lead.
- The headteacher/senior leaders will work with the responsible Governor, the designated safeguarding lead (DSL) and IT service providers in all aspects of filtering and monitoring.

Governors

Governors are responsible for the approval of the online safety policy and for reviewing the effectiveness of the policy. This will be carried out by the Governors receiving regular information about online safety incidents and monitoring reports. A member of the Governing Body has taken on the role of Online Safety Governor (Paul O'Connor-safeguarding governor)

The role of the Online Safety Governor will include:

[1] See flow chart on dealing with online safety incidents in 'Responding to incidents of misuse' and relevant local authority/MAT/ HR/other relevant body disciplinary procedures.

- annual meetings with the Online Safety Lead, alongside regular meetings with the DSL
- annual monitoring of online safety incident logs
- annual monitoring of filtering control logs
- reporting to other relevant Governors
- checking that provision outlined in the online safety policy is taking place as intended e.g. staff training, online safety education

Designated Safety Lead (DSL)

The DSL will:

- hold the lead responsibility for online safety, within their safeguarding role as stipulated in Keeping Children Safe in Education.
- Receive relevant and regularly updated training in online safety to enable them to understand the risks associated with online safety and be confident that they have the relevant knowledge and up to date capability required to keep children safe whilst they are online
- meet regularly with the online safety governor to discuss current issues, review (anonymised) incidents and filtering and monitoring logs and ensuring that annual (at least) filtering and monitoring checks are carried out
- attend relevant governing body meetings/groups
- report regularly to the senior leadership team
- be responsible for receiving reports of online safety incidents and handling them, and deciding whether to make a referral by liaising with relevant agencies, ensuring that all incidents are recorded.
- liaise with staff and IT providers on matters of safety and safeguarding and welfare (including online and digital safety)

Online Safety Lead

- work closely on a day-to-day basis with the Designated Safeguarding Lead (DSL),
- receive reports of online safety issues- via Content Keeper, being aware of the potential for serious child protection concerns and ensure that these are logged to inform future online safety developments
- have a leading role in establishing and reviewing the school online safety policies/documents
- promote an awareness of and commitment to online safety education / awareness raising across the school and beyond
- liaise with curriculum leaders to ensure that the online safety curriculum is planned, mapped, embedded and evaluated
- ensure that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place and the need to immediately report those incidents
- provide (or identify sources of) training and advice for staff/governors/parents/carers/learners
- liaise with local authority, technical staff, pastoral staff and support staff
- receive regularly updated training to allow them to understand how digital technologies are used and are developing (particularly by learners) with regard to the areas defined In Keeping Children Safe in Education:
    - content
    - contact

- conduct
- commerce

Curriculum Leads

Curriculum Leads will work with the DSL/OSL to develop a planned and coordinated online safety education programme
This will be provided through:

- a discrete programme -Twinkl
- PHSE and SRE programmes- SCARF
- assemblies and pastoral programmes
- through relevant national initiatives and opportunities e.g. Safer Internet Day and Anti-bullying week.

Network Manager/Technical staff - Trailblaze

Those with technical responsibilities are responsible for ensuring:

- they are aware of and follow the school Online Safety Policy and Technical Security Policy to carry out their work effectively in line with school policy
- **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 BCP online safety policy/guidance that may apply.**
- **that users may only access the networks and devices through a properly enforced password protection policy**

- the filtering policy is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person. The filtering list is a live updated daily list that comes from the government body (CAIC list)
- that they keep up to date with online safety technical information in order to effectively carry out their online safety role and to inform and update others as relevant
- that the use of the networks/internet/digital technologies is regularly monitored in order that any misuse/attempted misuse can be reported to the Headteacher and Senior Leaders; Online Safety Lead for investigation/action/*sanction* using Content Keeper
- that monitoring software/systems are implemented and updated as agreed in school policies- Content Keeper
- there is clear, safe, and managed control of user access to networks and devices

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 understand that online safety is a core part of safeguarding
- they have read, understood and signed the staff acceptable use policy (AUP)
- they follow all relevant guidance and legislation including, for example, Keeping Children Safe in Education and UK GDPR regulations
- all digital communications with learners, parents and carers and others should be on a professional level and only carried out using official school systems and devices (where staff use AI, they should only use school-approved AI services for work

purposes which have been evaluated to comply with organisational security and oversight requirements

- they report any suspected misuse or problem by a child to the Headteacher or DSL via My Concern for investigation/action/sanction
- they report any suspected misuse or problem by an adult to the Headteacher for investigation/action/sanction
- 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.
- where lessons take place using live-streaming or video-conferencing, there is regard to national safeguarding guidance and local safeguarding policies (n.b. the guidance contained in the SWGfL Safe Remote Learning Resource
- there is a zero-tolerance approach to incidents of online-bullying, sexual harassment, discrimination, hatred etc
- they model safe, responsible, and professional online behaviours in their own use of technology, including out of school and in their use of social media.
- they adhere to the school's technical security policy, with regard to the use of devices, systems and passwords and have an understanding of basic cybersecurity
- they have a general understanding of how the learners in their care use digital technologies out of school, in order to be aware of online safety issues that may develop from the use of those technologies
- they are aware of the benefits and risks of the use of Artificial Intelligence (AI) services in school, being transparent in how they use these services, prioritising human oversight. AI should assist, not replace, human decision-making. Staff must ensure that final judgments, particularly those affecting people, are made by humans, fact-checked and critically evaluated.

Pupils are taught to:

- be responsible for using the school digital technology systems in accordance with the pupil acceptable use policy
- should know what to do if they or someone they know feels vulnerable when using online technology.
- should avoid plagiarism and uphold copyright regulations, taking care when using Artificial Intelligence (AI) services to protect the intellectual property of themselves and others and checking the accuracy of content accessed through AI services.
- understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- 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.

- 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:

- Providing them with a copy of the Acceptable Use policy for pupils (Home school book)
- Publishing the Online Safety policy on the school website
- parents' evenings, Marvellous Me, newsletters, letters, website, social media and information about national/local online safety campaigns/literature.
- Seeking their permission concerning digital images

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
- the use of Microsoft Teams for remote learning purposes
- reinforcing the online safety messages provided to their children in school

Professional Standards

There is an expectation that professional standards will be applied to online safety as in other aspects of school life i.e.

- there is a consistent emphasis on the central importance of literacy, numeracy, digital competence and digital resilience. Learners will be supported in gaining skills across all areas of the curriculum and every opportunity will be taken to extend learners' skills and competence
- there is a willingness to develop and apply new techniques to suit the purposes of intended learning in a structured and considered approach and to learn from the experience, while taking care to avoid risks that may be attached to the adoption of developing technologies e.g. Artificial Intelligence (AI) tools.
- Staff are able to reflect on their practice, individually and collectively, against agreed standards of effective practice and affirm and celebrate their successes
- policies and protocols are in place for the use of online communication technology between the staff and other members of the school and wider community, using officially sanctioned school mechanisms.

Policy Statements

Education –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 should be provided as part of Computing lessons and should be regularly revisited**
- **Key online safety messages should be reinforced as part of a planned programme of assemblies and pastoral activities**
- **Pupils should be taught in all lessons to be critically aware of the materials/content they access on-line and be guided to validate the accuracy of information.**
- **Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet (UKS2)**
- **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.**
- **learners should be taught in all lessons to be critically aware of the materials/content they access online and be guided to validate the accuracy of information (including where the information is gained from Artificial Intelligence services)**
- **learners should be taught to acknowledge the source of information used and to respect copyright / intellectual property when using material accessed on the internet and particularly through the use of Artificial Intelligence services**
- 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 students/pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.
- Where pupils are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit. - including AI systems
- It is accepted that from time to time, for good educational reasons, students may need to research topics (e.g. racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Technical Staff (Trailblaze via Deputy Headteacher or Online Safety Lead) can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need.

Education – Parents/carers

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

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

- Curriculum activities
- Letters, newsletters, via Marvellous Me
- Parents/carers evenings
- High profile events/campaigns e.g. Safer Internet Day

- Reference to the relevant web sites/publications e.g. swgfl.org.uk, www.saferinternet.org.uk/, http://www.childnet.com/parents-and-carers (see appendix for further links/resources)

Education & Training – Staff/Volunteers

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

- **A planned programme of formal regular online safety training will be made available to staff. This will be regularly updated and reinforced.**
- **Online safety training is included as part of the induction programme for new staff, ensuring that they fully understand the school/academy online safety policy and acceptable use agreements.**
- **the training will be an integral part of the school's annual safeguarding, data protection and cyber-security training for all staff**
- It is expected that some staff will identify online safety as a training need within the performance management process.
- The Online Safety Lead will receive regular updates through attendance at external training events (e.g. 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.
- The Online Safety Lead will provide advice/guidance/training to individuals as required.

Training – Governors

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

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

A higher level of training will be made available to (at least) the Online Safety Governor. This will include:

- Cyber-security training (at least at a basic level)
- Training to allow the governor to understand the school's filtering and monitoring provision, in order that they can participate in the required checks and reviews.

The use of Artificial Intelligence (AI) systems in School

As Generative Artificial Intelligence (gen AI) continues to advance and influence the world we live in, its role in education is also evolving. There are currently 3 key dimensions of AI use in schools: learner support, teacher support and school operations; ensuring all use is safe, ethical and responsible is essential.

We realise that there are risks involved in the use of Gen AI services, but that these can be mitigated through our existing policies and procedures, amending these as necessary to address the risks.

We will educate staff and learners about safe and ethical use of AI, preparing them for a future in which these technologies are likely to play an increasing role.

The safeguarding of staff and learners will, as always, be at the forefront of our policy and practice.

Policy Statements

- The school acknowledges the potential benefits of the use of AI in an educational context - including enhancing learning and teaching, improving outcomes, improving administrative processes, reducing workload and preparing staff and learners for a future in which AI technology will be an integral part. Staff are encouraged to use AI based tools to support their work where appropriate, within the frameworks provided below and are required to be professionally responsible and accountable for this area of their work.
- **We will comply with all relevant legislation and guidance, with reference to guidance contained in Keeping Children Safe in Education and UK GDPR**
- **We will provide relevant training for staff and governors in the advantages, use of and potential risks of AI. We will support staff in identifying training and development needs to enable relevant opportunities**.
- **We will seek to embed learning about AI as appropriate in our curriculum offer, including supporting learners to understand how gen AI works, its potential benefits, risks, and ethical and social impacts. The school recognises the importance of equipping learners with the knowledge, skills and strategies to engage responsibly with AI tools...**
- **As set out in the staff acceptable use agreement, staff will be supported to use AI tools responsibly, ensuring the protection of both personal and sensitive data. Staff should only input anonymised data to avoid the exposure of personally identifiable or sensitive information.**
- **Staff will always ensure AI tools used comply with UK GDPR and other data protection regulations. They must verify that tools meet data security standards before using them for work related to the school.**
- **Only those AI technologies approved by the school may be used. Staff should always use school-provided AI accounts for work purposes. These accounts are configured to comply with organisational security and oversight requirements, reducing the risk of data breaches.**
- **We will protect sensitive information. Staff must not input sensitive information, such as internal documents or strategic plans, into third-party AI tools unless explicitly vetted for that purpose. They must always recognise and safeguard sensitive data.**
- **The school will ensure that when AI is used, it will not infringe copyright or intellectual property conventions – care will be taken to avoid intellectual property, including that of the learners, being used to train generative AI models without appropriate consent.**
- **AI incidents must be reported promptly. Staff must report any incidents involving AI misuse, data breaches, or inappropriate outputs immediately to the relevant internal teams. Quick reporting helps mitigate risks and facilitates a prompt response.**
- The school will audit all AI systems in use and assess their potential impact on staff, learners and the school's systems and procedures, creating an AI inventory listing all

tools in use, their purpose and potential risks. (Risk assessment matrices are attached as an appendix)

- We are aware of the potential risk for discrimination and bias in the outputs from AI tools and have in place interventions and protocols to deal with any issues that may arise. When procuring and implementing AI systems, we will follow due care and diligence to prioritise fairness and safety.
- The school will support parents and carers in their understanding of the use of AI in the school (this could be through an "AI in our school guide")
- AI tools may be used to assist teachers in the assessment of learners' work, identification of areas for improvement and the provision of feedback. Teachers may also support learners to gain feedback on their own work using AI
- Maintain Transparency in AI-Generated Content. Staff should ensure that documents, emails, presentations, and other outputs influenced by AI include clear labels or notes indicating AI assistance. Clearly marking AI-generated content helps build trust and ensures that others are informed when AI has been used in communications or documents.
- We will prioritise human oversight. AI should assist, not replace, human decision-making. Staff must ensure that final judgments, particularly those affecting people, are made by humans and critically evaluate AI-generated outputs. They must ensure that all AI-generated content is fact-checked and reviewed for accuracy before sharing or publishing. This is especially important for external communication to avoid spreading misinformation.
- Recourse for improper use and disciplinary procedures. Improper use of AI tools, including breaches of data protection standards, misuse of sensitive information, or failure to adhere to this agreement, will be subject to disciplinary action as defined in Staff Disciplinary Policy.

Technical – infrastructure/equipment, filtering and monitoring

- **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 users will be provided with a username and secure password by Trailblaze who will keep an up to date record of users and their usernames. Users are responsible for the security of their username and password**.
- The "administrator" passwords for the school systems, used by Trailblaze are kept by Trailblaze but will be made available to the Headteacher in the event we no longer require their services and will be kept in a secure place
- Trailblaze work with the school to ensure 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 and monitored for all users.** Illegal content (e.g. 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. Any filtering changes

logged with Trailblaze are actioned within 24 hours under the schools SLA agreement.

- **Devices that are provided by the school have school-based filtering applied irrespective of their location.**
- **Internet filtering/monitoring should ensure that children are safe from terrorist and extremist material when accessing the internet.**
- The school does not currently have split staff/student filtering but this can be requested if the need arises.
- Trailblaze regularly monitor and record the activity of users on the school technical systems and users are made aware of this in the acceptable use agreement.
- An appropriate system is in place for users to report any actual/potential technical incident/security breach to the relevant person, as agreed).
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, mobile devices, etc. from accidental or malicious attempts which might threaten the security of the school systems and data. These are tested regularly. The school infrastructure and individual devices are protected by up to date virus software.
- An agreed Acceptable Use policy is in place for the provision of temporary access of "guests" (e.g. trainee teachers, supply teachers, visitors) onto the school systems.
- An agreed Acceptable Use policy is in place regarding the extent of personal use that users (staff/students/pupils/community users) and their family members are allowed on school devices that may be used out of school.
- An agreed Acceptable Use policy is in place that allows staff to download executable files and installing programmes on school devices. This is monitored through Content Keeper and will be alerted if causing concern
- An agreed policy (GDPR)is in place regarding the use of removable media (e.g. memory sticks/CDs/DVDs) by users on school devices. **Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured**
- **The monitoring provision is reviewed at least once every academic year and updated in response to changes in technology and patterns of online safety incidents and behaviours. The review should be conducted by members of the senior leadership team, the designated safeguarding lead, and technical staff. It will also involve the responsible governor. The results of the review will be recorded and reported as relevant.**

- **Mobile Technologies - See Mobile Technology policy**

  Mobile technology devices may be school owned/provided or personally owned and might include: smartphone, tablet, notebook/laptop or other technology that could have the capability of utilising the school's wireless network. The device then has access to the wider internet, cloud-based services such as email. (see table below for what is allowed)

  All users should understand that the primary purpose of the use mobile/personal devices in a school context is educational. The mobile technologies policy is consistent with and inter-related to other relevant school polices including but not limited to the safeguarding policy, behaviour policy, bullying policy, acceptable use policy, and policies around theft or malicious damage. Teaching about the safe and appropriate use of mobile technologies should be an integral part of the school's online safety education programme.

- **The school acceptable use agreements for staff, pupils/students and parents/carers will give consideration to the use of mobile technologies**
- **The school allows:**

	Personal Devices		
	Student owned	**Staff owned**	**Visitor owned**
Allowed in school	*Yes **	*YES*	*Yes*
Full network access	*NO*	*NO*	*NO*
Internet only	*NO*	*YES*	*YES*

* MOBILE PHONES ONLY-These are locked away in a school safe and given back to children at the end of the school day.

School owned/provided devices:

- Will be provided for staff to use in lessons and at home/off site
- Remote access to school network can be maintained on School laptops being used outside of the school premises
- Staff can add app's to iPad's if it is for an educational purpose and with no cost to the school
- Technical support – Any issues will be reported to Trailblaze via Helpdesk
- Filtering of devices- In line with school network
- Taking/storage/use of images-school devices can be used to take and store images for school use only
- Exit processes – Business Manager keeps a log of loaned devices and these are collected when a member of staff leaves and given to Trailblaze to reset if required
- Liability for damage- covered under school insurance
- Pupils are able to access the school's network and the internet using their own login information on school owned devices. This has limited access to the network and can be monitored by staff. The school owned devices are only to be used by children during lesson times unless special arrangements have been made with the class teacher e.g for use at playtimes/lunchtimes if injury does not allow the child to be outside.
- Children are supervised at all times whilst using school devices.

Personal devices:

- Staff and visitors are allowed to use personal mobile devices in school
- Personal devices must never be used when children are present
- Personal devices must be stored out of sight of children
- Staff will be allowed to use personal devices for school business
- There is NO technical support provided for personal devices.
- Filtering of the internet connection to these devices
- Data Protection
- School has the right to take, examine and search users' devices in the case of misuse
- The school will not accept liability for loss/damage or malfunction following access to the network
- Visitors will be informed about school requirements on arrival in school
- Children are not allowed to use ANY personal devices in the school day. As previously stated all pupil owned mobile phones are kept in a looked cupboard in the morning and given back to the child at the end of the school day.

Use of digital and video images

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

need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for online-bullying to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. It is common for employers to carry out internet searches for information about potential and existing employees. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- **When using digital images, staff should inform and educate students/pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.**
- **Written permission from parents or carers will be obtained before photographs of students/pupils are published on the school website/social media/local press**
- In accordance with guidance from the Information Commissioner's Office, parents/carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use in not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published/made publicly available on social networking sites, nor should parents/carers comment on any activities involving other pupils in the digital/video images.
- Staff and volunteers are allowed to take digital/video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment; the personal equipment of staff should not be used for such purposes.
- Care should be taken when taking digital/video images that 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.
- Pupil's work can only be published with the permission of the pupil and parents or carers.

Data Protection
Personal data will be recorded, processed, transferred and made available according to the current data protection legislation.

The school must ensure that:
- **it has a Data Protection Policy.**
- **it implements the data protection principles and is able to demonstrate that it does so through use of policies, notices and records.**
- **it has paid the appropriate fee Information Commissioner's Office (ICO) and included details of the Data Protection Officer (DPO).**
- **it has appointed an appropriate Data Protection Officer (DPO), who has a high level of understanding of data protection law and is free from any conflict of interest.**

- **it has an 'information asset register' in place and knows exactly what personal data it holds, where this data is held, why and which member of staff has responsibility for managing it**
- **the information asset register records the lawful basis for processing personal data (including, where relevant, how consent was obtained and refreshed). Where special category data is processed, an additional lawful basis will have also been recorded**
- **it will hold only the minimum personal data necessary to enable it to perform its function and it will not hold it for longer than necessary for the purposes it was collected for. The school should develop and implement a 'retention policy" to ensure there are clear and understood policies and routines for the deletion and disposal of data to support this. personal data held must be accurate and up to date where this is necessary for the purpose it is processed for. Have systems in place to identify inaccuracies, such as asking parents to check emergency contact details at suitable intervals**
- **it provides staff, parents, volunteers, with information about how the school/academy looks after their data and what their rights are in a clear Privacy Notice**
- **procedures must be in place to deal with the individual rights of the data subject, e.g. one of the 8 data subject rights applicable is that of Subject Access which enables an individual to see to have a copy of the personal data held about them (subject to certain exceptions which may apply).**
- **data Protection Impact Assessments (DPIA) are carried out where necessary. For example, to ensure protection of personal data when accessed using any remote access solutions, or entering into a relationship with a new supplier (this may also require ensuring that data processing clauses are included in the supply contract or as an addendum)**
- **Regular updates & patches are applied to the system, at Server & client level, this ensures all crucial systems are always up to date and secure against any attacks.**
- **it has undertaken appropriate due diligence and has required data processing clauses in contracts in place with any data processors where personal data is processed.**
- **it understands how to share data lawfully and safely with other relevant data controllers.**
- **it reports any relevant breaches to the Information Commissioner within 72hrs of becoming aware of the breach in accordance with UK data protection law. It also reports relevant breaches to the individuals affected as required by law. In order to do this, it has a policy for reporting, logging, managing, investigating and learning from information risk incidents.**
- **The school has a Freedom of Information Policy which sets out how we will deal with FOI requests.**
- **all staff receive data protection training at induction and appropriate refresher training thereafter. Staff undertaking particular data protection functions, such as handling requests under the individual's rights, will receive training appropriate for their function as well as the core training provided to all staff.**

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

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

Staff must ensure that they:

- **at all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse**
- **can recognise a possible breach, understand the need for urgency and know who to report it to within the school**

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

Cyber Security (new January 2025)

The DfE Cyber security standards for schools and colleges explains:

"Cyber incidents and attacks have significant operational and financial impacts on schools and colleges. These incidents or attacks will often be an intentional and unauthorised attempt to access, change or damage data and digital technology. They could be made by a person, group, or organisation outside or inside the school or college and can lead to:

- safeguarding issues due to sensitive personal data being compromised
- impact on student outcomes
- a significant data breach
- significant and lasting disruption, including the risk of repeated future cyber incidents and attacks, including school or college closure
- financial loss
- reputational damage"

- the school has reviewed the DfE Cyber security standards for schools and colleges and is working toward meeting these standards
- the school will conduct a cyber risk assessment annually and review each term
- the school, (*in partnership with Trailblaze),* has identified the most critical parts of the school's digital and technology services and sought assurance about their cyber security
- the school has an effective backup and restoration plan in place in the event of cyber attacks
- the school's governance and IT policies reflect the importance of good cyber security
- staff and Governors receive training on the common cyber security threats and incidents that schools experience
- the school's education programmes include cyber awareness for learners
- the school has a business continuity and incident management plan in place
- there are processes in place for the reporting of cyber incidents. All students and staff have a responsibility to report cyber risk or a potential incident or attack, understand how to do this feel safe and comfortable to do so.

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

	Staff & other adults				Students/Pupils			
Communication Technologies	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission	Not allowed
Mobile phones may be brought to the school	/				/			
Use of mobile phones in lessons				/				/
Use of mobile phones in social time		/						/
Taking photos on personal mobile phones/cameras				/				/
Use of other personal mobile devices e.g. tablets, gaming devices		/						/
Use of personal email addresses in school or on school network		/						/
Use of school email for personal emails				/				/
Use of messaging apps		/						/
Use of social media		/						/
Use of blogs		/						/

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

- **The official school email service may be regarded as safe and secure and is monitored. Users should be aware that email communications are monitored.**
- **Users must immediately report, to 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. (See Communication policy)**
- **Any digital communication between staff and pupils or parents/carers (email, social media, etc) must be professional in tone and content.** These communications may

only take place on official (monitored) school systems. Personal email addresses, text messaging or social media must not be used for these communications.
- students will be provided with individual school email addresses for educational use.
- pupils should be taught about online safety issues, such as the risks attached to the sharing of personal details. They should also be taught strategies to deal with inappropriate communications and be reminded of the need to communicate appropriately when using digital technologies.
- Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff.

Social Media - Protecting Professional Identity

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

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

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

Personal Use:

- Personal communications are those made via a personal social, media accounts. In all cases, where a personal account is used which associates itself with the school or impacts on the school, it must be made clear that the member of staff is not communicating on behalf of the school with an appropriate disclaimer. Such personal communications are within the scope of this policy
- Personal communications which do not refer to or impact upon the school are outside the scope of this policy
- Where excessive personal use of social media in school is suspected, and considered to be interfering with relevant duties, disciplinary action may be taken
- The school permits reasonable and appropriate access to private social media sites

Monitoring of Public Social Media:

- As part of active social media engagement, it is considered good practice to pro-actively monitor the Internet for public postings about the school
- The school should effectively respond to social media comments made by others according to a defined policy or process

Dealing with unsuitable/inappropriate activities

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

The school believes that the activities referred to in the following section would be inappropriate in a school context and that users, as defined below, should not engage in these activities in/or outside the school when using school equipment or systems. The school policy restricts usage as follows:

User Actions		Acceptable	Acceptable at certain times	Acceptable for nominated	Unacceptable	Unacceptable and illegal
Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	Child sexual abuse images –The making, production or distribution of indecent images of children. Contrary to The Protection of Children Act 1978					X
	Grooming, incitement, arrangement or facilitation of sexual acts against children Contrary to the Sexual Offences Act 2003.					X
	Possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character) Contrary to the Criminal Justice and Immigration Act 2008					X
	Criminally racist material in UK – to stir up religious hatred (or hatred on the grounds of sexual orientation) - contrary to the Public Order Act 1986					X
	Pornography				X	
	Promotion of any kind of discrimination					X
	threatening behaviour, including promotion of physical violence or mental harm					X
	Promotion of extremism or terrorism					X

	Any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute				X	
Activities that might be classed as cyber-crime under the Computer Misuse Act: • Gaining unauthorised access to school networks, data and files, through the use of computers/devices • Creating or propagating computer viruses or other harmful files • Revealing or publicising confidential or proprietary information (e.g. financial / personal information, databases, computer / network access codes and passwords) • Disable/Impair/Disrupt network functionality through the use of computers/devices • Using penetration testing equipment (without relevant permission) • Using another individual's username and password to access data, a program or parts of the system that the user is not authorised to access						X
Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school					X	
Revealing or publicising confidential or proprietary information (e.g. financial/personal information, databases, computer/network access codes and passwords)					X	
Unfair usage (downloading/uploading large files that hinders others in their use of the internet)					X	
Using school systems to run a private business					X	
Infringing copyright					X	
On-line gaming (educational)	x					
On-line gaming (non-educational)		x				
On-line gambling					x	
On-line shopping/commerce				x		
File sharing	x					
Use of social media				x		
Use of messaging apps				x		
Use of video broadcasting e.g. YouTube				x		
Use of AI services that have NOT been approved by the school					x	

Reporting and responding

The school will take all reasonable precautions to ensure online safety for all school users but recognises that incidents may occur inside and outside of the school (with impact on the school) which will need intervention. The school will ensure:

- **there are clear reporting routes which are understood and followed by all members of the school community which are consistent with the school safeguarding procedures, and with the whistleblowing, complaints and managing allegations policies.**
- **all members of the school community will be made aware of the need to report online safety issues/incidents**
- **reports will be dealt with as soon as is practically possible once they are received**
- **the Designated Safeguarding Lead, Online Safety Lead and other responsible staff have appropriate skills and training to deal with online safety risks.**
- **if there is any suspicion that the incident involves any illegal activity or the potential for serious harm the incident must be escalated through the agreed school safeguarding procedures, this may include**

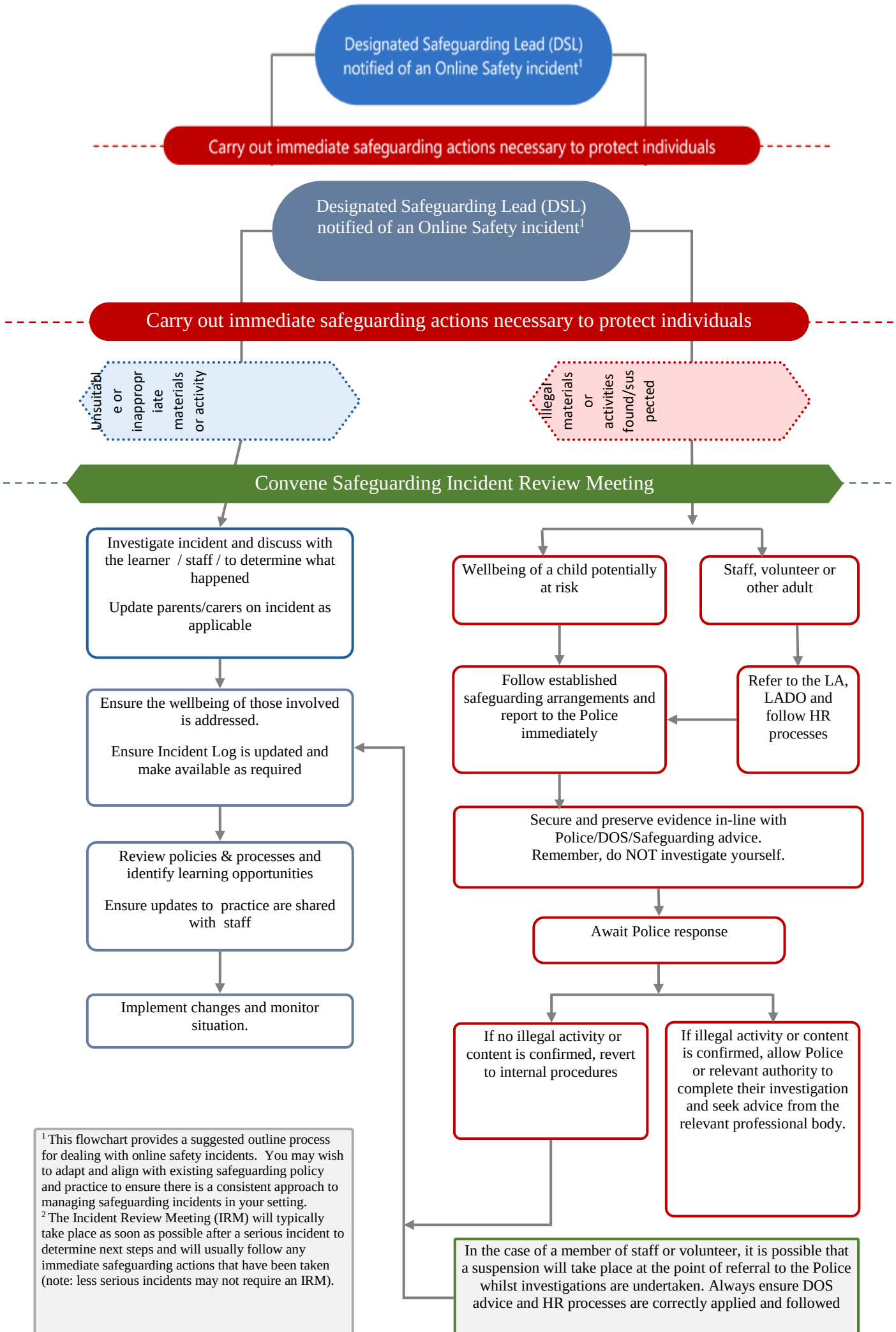
    - Non-consensual images
    - Self-generated images
    - Terrorism/extremism
    - Hate crime/ Abuse
    - Fraud and extortion
    - Harassment/stalking
    - Child Sexual Abuse Material (CSAM)
    - Child Sexual Exploitation Grooming
    - Extreme Pornography
    - Sale of illegal materials/substances
    - Cyber or hacking offences under the Computer Misuse Act
    - Copyright theft or piracy

- any concern about staff misuse will be reported to the Headteacher, unless the concern involves the Headteacher, in which case the complaint is referred to the Chair of Governors and the local authority
- where AI is used to support monitoring and incident reporting, human oversight is maintained to interpret nuances and context that AI might miss
- where there is no suspected illegal activity, devices may be checked using the following procedures:
    - one or more senior members of staff should be involved in this process. This is vital to protect individuals if accusations are subsequently reported.
    - conduct the procedure using a designated device that will not be used by learners and, if necessary, can be taken off site by the police should the need arise (should illegal activity be subsequently suspected). Use the same device for the duration of the procedure.
    - ensure that the relevant staff 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

    - 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 / MAT (as relevant)
        - police involvement and/or action
- it is important that those reporting an online safety incident have confidence that the report will be treated seriously and dealt with effectively
- there are support strategies in place e.g., peer support for those reporting or affected by an online safety incident
- incidents should be logged (Arbor)
- relevant staff are aware of external sources of support and guidance in dealing with online safety issues, e.g. local authority; police; Professionals Online Safety Helpline; Reporting Harmful Content; CEOP.
- those involved in the incident will be provided with feedback about the outcome of the investigation and follow up actions (as relevant)
- learning from the incident (or pattern of incidents) will be provided (as relevant and anonymously) to:
    - the Online Safety lead for consideration of updates to policies or education programmes and to review how effectively the report was dealt with
    - staff, through regular briefings
    - learners, through assemblies/lessons
    - parents/carers, through newsletters, school social media, website
    - governors, through regular safeguarding updates
    - local authority/external agencies, as relevant the school will make the flowchart below available to staff to support the decision-making process for dealing with online safety incidents.

Illegal Incidents

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


Designated Safeguarding Lead (DSL) notified of an Online Safety incident[1]
Carry out immediate safeguarding actions necessary to protect individuals
Designated Safeguarding Lead (DSL) notified of an Online Safety incident[1]
Carry out immediate safeguarding actions necessary to protect individuals
Unsuitable or inappropriate materials or activity
Illegal materials or activities found/suspected
Convene Safeguarding Incident Review Meeting
Investigate incident and discuss with the learner / staff / to determine what happened
Update parents/carers on incident as applicable
Ensure the wellbeing of those involved is addressed.
Ensure Incident Log is updated and make available as required
Review policies & processes and identify learning opportunities
Ensure updates to practice are shared with staff
Implement changes and monitor situation.
Wellbeing of a child potentially at risk
Staff, volunteer or other adult
Follow established safeguarding arrangements and report to the Police immediately
Refer to the LA, LADO and follow HR processes
Secure and preserve evidence in-line with Police/DOS/Safeguarding advice.
Remember, do NOT investigate yourself.
Await Police response
If no illegal activity or content is confirmed, revert to internal procedures
If illegal activity or content is confirmed, allow Police or relevant authority to complete their investigation and seek advice from the relevant professional body.
In the case of a member of staff or volunteer, it is possible that a suspension will take place at the point of referral to the Police whilst investigations are undertaken. Always ensure DOS advice and HR processes are correctly applied and followed
[1] This flowchart provides a suggested outline process for dealing with online safety incidents. You may wish to adapt and align with existing safeguarding policy and practice to ensure there is a consistent approach to managing safeguarding incidents in your setting.
[2] The Incident Review Meeting (IRM) will typically take place as soon as possible after a serious incident to determine next steps and will usually follow any immediate safeguarding actions that have been taken (note: less serious incidents may not require an IRM).

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:

	Actions/Sanctions								
Students/Pupils Incidents	Refer to class teacher	Refer to Phase Leader	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 e.g. Internal or external exclusion
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable/inappropriate activities).			X	X					x
Unauthorised use of non-educational sites during lessons	x	x			x	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		x	
Attempting to access or accessing the school network, using another pupil's account	x	x						x	
Attempting to access or accessing the school network, using the account of a member of staff		x				x			x
Corrupting or destroying the data of other users			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

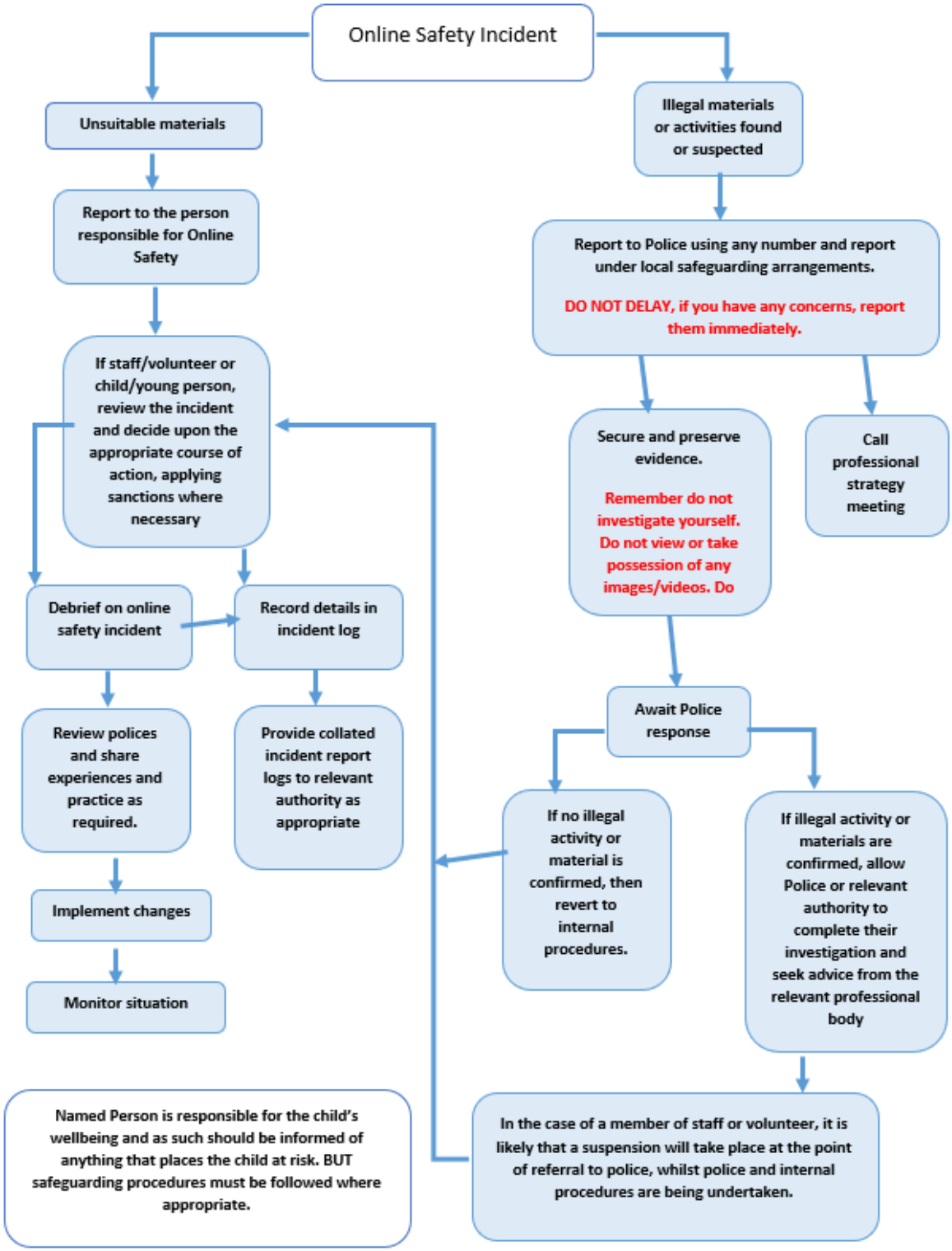
Actions which could bring the school/academy into disrepute or breach the integrity of the ethos of the school			x			x			x
Using proxy sites or other means to subvert the school's/academy's filtering system			x		x	x			x
Accidentally accessing offensive or pornographic material and failing to report the incident			x		x			x	
Deliberately accessing or trying to access offensive or pornographic material			x	x		x			x
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act			x	x		x			x

Actions/Sanctions

Staff Incidents	Refer to line manager	Refer to Headteacher	Refer to LADO/HR	Refer to Police	Refer to Technical Support Staff for action re filtering	Warning	Suspension	Disciplinary action
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable/inappropriate activities).		X	X	X				x
Inappropriate personal use of the internet/social media/personal email		x	x			x		
Unauthorised downloading or uploading of files		x						
Allowing others to access school network by sharing username and passwords or attempting to access or accessing the school network, using another person's account		x			x	x		
Careless use of personal data e.g. holding or transferring data in an insecure manner		x						
Deliberate actions to breach data protection or network security rules		x				x		
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software		x			x	x		

Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature		x	x					x
Using personal email/social networking/instant messaging/text messaging to carrying out digital communications with students/pupils		x	x					
Actions which could compromise the staff member's professional standing		x	x					
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school		x	x					
Using proxy sites or other means to subvert the school's filtering system		x			x			
Accidentally accessing offensive or pornographic material and failing to report the incident		x	x		x	x		
Deliberately accessing or trying to access offensive or pornographic material		x	x	x				x
Breaching copyright or licensing regulations		x						
Continued infringements of the above, following previous warnings or sanctions		X						x

Responding to incidents of misuse – flow chart



Record of reviewing devices/internet sites (responding to incidents of misuse)

Group: .....
Date: .....
Reason for investigation: .....
.....
.....

Details of first reviewing person

Name: .....
Position: .....
Signature: .....

Details of second reviewing person

Name: .....
Position: .....
Signature: .....

Name and location of computer used for review (for web sites)

.....
.....

Web site(s) address/device	Reason for concern

Conclusion and Action proposed or taken

Reporting Log

Group: .....

Date	Time	Incident	Action Taken		Incident Reported By	Signature
			What?	By Whom?		

Training Needs Audit Log

Group: .....

Relevant training the last 12 months	Identified Training Need	To be met by	Cost	Review Date