On-line Safety Policy

Rewritten and updated to fulfil KCSIE requirements
Version 2 - 2024

Full Governing Body
Date approved:

Development / Monitoring / Review of this Policy

This Online Safety policy has been developed by the Online Safety Coordinator in close working relationship with the school's Designated Safeguarding Lead.

Schedule for Development / Monitoring / Review

This Online Safety policy was approved by the Governing Body / Governors Sub Committee on:	
The implementation of this Online Safety policy will be monitored by the Online Safety Coordinator	*Online Safety Co-ordinator*
Monitoring will take place at regular intervals:	*Annually*
The Governing Body / Governors Sub Committee will receive a report on the implementation of the Online Safety Policy generated by the Online Safety Coordinator (which will include anonymous details of online safety incidents) at regular intervals:	*After implementation, and at least annually.*
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:	
Should serious online safety incidents take place, the following external persons / agencies should be informed:	*School DSL* *Headteacher* *Starting Point* *LADO*

The school will monitor the impact of the policy using:

- logs of reported incidents
- monitoring logs of internet activity (including sites visited) / filtering
- internal monitoring data for network activity
- surveys / questionnaires of
    - students
    - parents / carers
    - staff

Scope of the Policy

This policy applies to all members of the school community (including staff, students, volunteers, parents / carers, visitors, community users) who have access to and are users of school digital technology systems, both in and out of the school. It also applies to the use of personal digital technology on the school site.

Roles and Responsibilities

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

Governors

Governors are responsible for the approval of the Online Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the Governors through the Education Committee receiving regular information about online safety incidents and monitoring reports.

A member of the Governing Body has taken on the role of Online Safety Governor. The role of the Online Safety Governor will include:

- regular meetings with the Online Safety Coordinator
- regular monitoring of online safety incident logs
- regular monitoring of filtering / change control logs
- reporting to relevant Governors / Committee / meeting
- ensuring that the filtering and monitoring provision is reviewed and recorded, at least annually.

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, defined in Keeping Children Safe in Education.
- the Headteacher and DSL 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.
- the Headteacher and DSL are responsible for ensuring that the Online Safety Coordinator and other relevant staff receive suitable training to enable them to carry out their online safety roles and to train other colleagues, as relevant.
- the Headteacher and DSL will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal online safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.
- the DSL will receive regular monitoring reports from the Online Safety Coordinator.
- the DSL will work with the responsible online safety governor to ensure the IT service team has a system in place which fulfils all aspects of filtering and monitoring requirements.

Online Safety Coordinator

- works closely with the DSL on current online safety issues and has a leading role in establishing and reviewing the school online safety policies / documents
- ensures that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place.
- provides training and advice for staff.
- liaises with the Local Authority and other relevant bodies e.g., South West Grid for Learning (SWGfL), East Midlands Cybersecurity Division (Police)
- liaises with school IT support staff, teaching staff and support staff.
- receives reports of online safety incidents and creates a log of incidents to inform future online safety developments
- meets regularly with Online Safety Governor to discuss current issues, review incident logs and filtering / change control logs
- attends relevant meeting / governors committee
- reports regularly to Senior Leadership Team
- 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

Network Manager / IT Support staff

The Network Manager and IT Support Staff are responsible for ensuring:

- that the school's technical infrastructure is secure and is not open to misuse or malicious attack
- that the school meets required online safety technical requirements and any Local Authority / Online Safety Policy / Guidance that may apply.
- that users may only access the networks and devices through a properly enforced password protection policy
- the filtering policy is applied and updated on a regular basis and that its implementation is not the sole responsibility of any one single person
- that they keep up to date with online safety technical information in order to effectively carry out their online safety role and to inform and update others as relevant
- that the use of the network / internet / Learning Platform / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the DSL for investigation / action / sanction
- that monitoring software / systems are implemented and updated as agreed in school policies

Teaching and Support Staff

Are responsible for ensuring that:

- they have an up to date awareness of online safety matters and of the current school Online Safety Policy and practices
- they understand that online safety is a core part of safeguarding
- they have read, understood and signed the Staff Acceptable Use Policy / Agreement (AUP)
- they report any suspected misuse or problem to the DSL for investigation / action / sanction
- all digital communications with students / parents / carers should be on a professional level and only carried out using official school systems
- online safety issues are embedded in all aspects of the curriculum and other activities
- students understand and follow the Online Safety Policy and acceptable use policies
- students have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- they monitor the use of digital technologies, mobile devices, cameras etc in lessons and other school activities (where allowed) and implement current policies with regard to these devices
- in lessons where internet use is pre-planned students 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.
- 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.

Designated Safeguarding Leads (DSLs)

The DSLs will be trained in Online Safety issues and be aware of the potential for serious child protection / safeguarding issues to arise from:

- hold the lead responsibility for online safety, within their safeguarding role.
- provide induction training to staff on filtering and monitoring procedures in school.
- receive relevant and regularly updated training in online safety to enable them to understand the risks associated with online safety and to be confident that they have the relevant knowledge and up to date capability required to keep children safe whilst 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.
- report regularly to the headteacher.
- 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 technical support team on matters of safety and safeguarding and welfare (including online and digital safety)

Students

- are responsible for using the school's digital technology systems in accordance with the Student Acceptable Use Policy
- have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- should know what to do if they or someone they know feels vulnerable when using online technology.
- will be expected to know and understand policies on the use of mobile phones, entertainment and communication devices. They should also know and understand policies on the taking / use of images and on online-bullying.
- should understand the importance of adopting good online safety practices when using digital technologies out of school and realise that the school's Online Safety Policy covers their actions out of school, if related to their membership of the school.

Parents / Carers

Parents / Carers play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way. The school will take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website / Learning Platform and information about national / local online safety campaigns / literature. The Online Safety section of the school website will provide signposting to help and support.

Parents and carers will be encouraged to support the school in promoting good online safety practice and to follow guidelines on the appropriate use of:

- digital and video images taken at school events
- access to parents' /carers' sections of the website / Learning Platform and on-line student records
- their children's personal devices in the school

Policy Statements

Education – Students

Whilst regulation and technical solutions are very important, their use must be balanced by educating students to take a responsible approach. The education of students 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 / PSE / other lessons and should be regularly revisited
- key online safety messages should be reinforced as part of a planned programme of assemblies and tutorial / pastoral activities
- students 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.
- students should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- students 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.
- students should be helped to understand the need for the student Acceptable Use Policy 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 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 students are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites young people visit.
- it is accepted that from time to time, for good educational reasons, students may need to research topics (e.g. racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the IT Network Manager 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, website (Online Safety section) , Learning Platform
- parents / Carers events
- reference to the relevant websites / publications e.g. swgfl.org.uk www.saferinternet.org.uk/ http://www.childnet.com/parents-and-carers , https://www.vodafone.co.uk/mobile/digital-parenting

Education – The Wider Community

The school will provide opportunities for local community groups / members of the community to gain from the school's online safety knowledge and experience. This may be offered through the following:

- online safety messages targeted towards grandparents and other relatives as well as parents.
- the school website will provide online safety information for the wider community

Education & Training – Staff / Volunteers

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

- a planned programme of formal online safety training will be made available to staff. This will be regularly updated and reinforced. An audit of the online safety training needs of staff will be carried out as part of the annual S175 Safeguarding Audit.
- all new staff should receive online safety training as part of their induction programme, ensuring that they fully understand the school Online Safety Policy and Acceptable Use Policy.
- the Online Safety Coordinator 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 / team meetings / INSET days.
- the Online Safety Coordinator will provide advice / guidance / training to individuals as required.

Training – Governors

Governors should have the opportunity to take part in online safety training / awareness sessions, with particular importance for those who are members of any subcommittee / group involved in technology / online 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, The Key for School Governors).
- participation in school / training / information sessions for staff or parents

Filtering and Monitoring

The school filtering and monitoring provision is agreed by senior leaders, governors and the IT technical support team and is regularly reviewed (at least annually) and updated in response to changes in technology and patterns of online safety incidents/behaviours.

Day to day management of filtering and monitoring systems requires the specialist knowledge of both safeguarding and IT staff to be effective. The DSL will have lead responsibility for safeguarding and online safety and the IT technical support team will have technical responsibility.

The filtering and monitoring provision is reviewed (at least annually) by senior leaders, DSL and governors with the involvement of the IT technical support team, in particular when a safeguarding risk is identified, there is a change in working practice, e.g. remote access of when new technology is introduced.

Filtering

- the school manages access to content across its systems for all users and on all devices using the school's internet provision. The filtering provided meets the standards defined in the DfE Filtering standards for school and colleges and guidance provided in the UK Safer Internet Centre appropriate filtering.
- illegal content (e.g. child sexual abuse images) is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation URL list and the police accessed list of unlawful terrorist content, produced on behalf on the Home Office. Content lists are regularly updated.
- there are established and effective routes for users to report inappropriate content, recognising that no system can be 100% effective.
- there is a clear process in place to deal with, and log, requests/approvals for filtering changes
- filtering logs are regularly reviewed and alert the DSL to breaches of filtering policy, which are acted upon.

Monitoring

The school has monitoring systems in place to protect the school, systems and users:

- the school monitors all network use across all its devices and services.
- monitoring reports are urgently picked up, acted on and outcomes recorded by the DSL, and users are aware that the network (and devices) are monitored.
- there are effective protocols in place to report abuse/misuse. There is a clear process for prioritising response to alerts that require rapid safeguarding intervention.
- management of serious safeguarding alerts is consistent with safeguarding policy and practice.

The school follows the UK Safer Internet Centre Appropriate Monitoring guidance and protects users and school systems through the use of the appropriate blend of strategies informed by the school's risk assessment. These may include:

- physical monitoring (adult supervision in classroom and when using devices)
- internet use is logged, regularly monitored and reviewed.
- filtering logs are regularly analysed and breaches are reported to senior leaders
- pro-active alerts inform the school of breaches to filtering policy, allowing effective intervention
- where possible, school technicians regularly monitor the activity on school technical systems

Technical Security

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

- school IT 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 IT 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 IT Network Manager who will keep an up to date record of users and their usernames. Users are responsible for the security of their username and password and will be required to change their password regularly
- the “master / administrator” passwords for the school IT systems, used by the Network Manager must also be available to the Headteacher and kept in a secure place (e.g. school safe)
- the IT Network Manager is responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations.
- internet access is filtered for all users. Illegal content (child sexual abuse images) is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list. Content lists are regularly updated and internet use is logged and regularly monitored. There is a clear process in place to deal with requests for filtering changes.
- Internet filtering / monitoring should ensure that children are safe from terrorist and extremist material when accessing the internet.
- the school provides enhanced / differentiated user-level filtering (allowing different filtering levels for different groups of users – staff / students etc)
- school technical staff regularly monitor and record the activity of users on the school IT systems and users are made aware of this in the Acceptable Use Policy.
- 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 workstations are protected by up to date virus software.
- the network manager is responsible for ensuring that software purchased by and used by the school is adequately licenced and that the latest software updates (patches) are applied.
- there are rigorous and verified back-up routines, including the keeping of network-separated (air-gapped) copies off-sties or in the cloud
- procedures are in place for the provision of temporary access of “guests” (e.g. trainee teachers, supply teachers, visitors) onto the school systems.
- use of school devices out of school by family members is regulated by the school acceptable use policy statement that a user consents to when the device allocated to them
- personal use of any device on the school network is regulated by acceptable use statements that a user consents to when using the network.
- staff members are not permitted to install software on school-owned devices without the consent of the IT support team
- systems are in place to control and protect personal data and data is encrypted at rest and in transit.

Mobile Technologies, including Bring Your Own Device/Bring Your Own Technology (BYOD/BYOT)

Mobile technology devices may be school owned/provided or personally owned and might include: smartphone, tablet, notebook / laptop or other technology that usually has the capability of utilising the school’s wireless network. The device then has access to the wider internet, which may include the school’s learning platform and other cloud- based services such as email and data storage. Access to the school network or the internet on a device not owned by the school can only be granted by the IT Network Manager if they deem this necessary.

All users should understand that the primary purpose of the use mobile / personal devices in a school context is educational. The mobile technologies policy should be consistent with and interrelated to other relevant school polices including but not limited to the Child Protection and Safeguarding Policy, Behaviour Policy, Anti-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 Policies for staff, students and parents / carers will consider the use of mobile technologies**.**

Outside school

Where staff are interacting with children online, they will continue to follow the school's existing staff Code of Conduct.

It is important that all staff who interact with children, including online, continue to look out for signs a child may be at risk. Any such concerns should be dealt with as per the Child Protection and Safeguarding Policy and where appropriate referrals should still be made to Children's Social Care (tel.01629 533190) and the Police (tel.999/101). Staff may refer directly, although usually a referral would be made via the Designated Safeguarding Leads in the Student Wellbeing Team.

Online teaching will follow the same principles as set out in the staff Code of Conduct Policy, the On-line Safety in a Digital World Policy and the Acceptable Use Policy. The school will heed Department for Education guidance relating to online safety.

The school will ensure any use of online learning tools and systems is in line with privacy and data protection/GDPR requirements. The school has undertaken a Data Protection Impact Assessment (DPIA) screening document, provided by Derbyshire County Council and signed by the school Data Protection Officer (DPO). Schools have a choice about whether or not to use video/audio conferencing as part of remote learning. Please see the school's Remote Learning Plan on our website for an overview of remote learning provision.

Staff will consider guidance as detailed below when delivering virtual (remote learning) lessons, especially where webcams are involved:

- video/audio conferencing is permitted, using Google Meet, for one to one or group staff meetings and with groups of students. The purpose will be for remote learning and/or pastoral communication.
- staff should never perform <u>one-to one</u> video/audio conferencing with students, except in extreme safeguarding situations * (please see below, Safeguarding and Child Protection Provisions).
- staff who choose to make a live or pre-recorded video lesson must ensure that they think carefully about the background used in the video and should preferably blur the background or use a wall/area of their home that does not give away details about their home or location.
- before making a live or pre-recorded video lesson staff should ensure that location tracking is turned off on their device so that no location meta data is recorded in the video file.
- language used by staff in a live or pre-recorded video lesson must be professional and appropriate, and there should not be any staff family members or pets visible in the video.
- staff and children must wear suitable clothing, as should anyone else in the household.

- staff should make expectations for student behaviour clear in any live video/audio conference. If staff have concerns about live video or audio conferencing with a group of students, they may want to include more than one member of staff. Staff may terminate the conference if necessary.
- best practice for live video/audio conferencing would be for the student to be in a room with an open door, with a parent or trusted adult on the premises.
- the live class should not be recorded.
- staff should record, the length, time, date and attendance of any sessions held.
- staff must only use communication systems provided by the school to communicate with students. Any pre-recorded video lessons must only be uploaded and shared via staff accounts on Google Classroom. Any live video/audio conferencing with school students must be via Google Meet using staff school accounts to student school accounts logged in to the @belperschool.co.uk or @students.belperschool.co.uk domains.
- pre-recorded and live video lessons should be kept to a reasonable length of time, or the streaming may prevent the family or students from 'getting on' with their day.

Safeguarding and Child Protection Provisions

When staff nominated by the Headteacher or the Senior Designated Safeguarding Lead have been allocated particular responsibility for regularly checking in with EHCP/vulnerable students as part of a Contact Plan/tracking spreadsheet , then with parental/carer permission those members of staff may speak 1:1 with a student on a voice call In these circumstances, the phone call should be made to the student's parent/carer using a school landline or school mobile phone and then the member of staff should ask the parent/carer if they can speak to the student.

If the nominated member of staff cannot access a school phone, they may use a personal phone to call parents/carers, but only if they block their number so that personal contact details are not visible. The staff member would then ask parental /carer permission to speak to the student.

Staff performing this checking in task may use staff email accounts to email students on their student accounts. Personal email addresses must not be used by staff or students.

The purpose of such a phone call would be to check that a child is safe and well.

*In some rare safeguarding situations, it may be necessary for members of our school Child Protection Team to use video/audio conferencing with a student (using school accounts only on both sides) to check on child safety and welfare, where inclusion of the student's parent/carer may be detrimental to child safety. In this situation the Senior Designated Safeguarding Lead or Deputies would first seek advice from Police/colleagues at Children's Services and then notify the Headteacher. There may be helpful safeguards such as including an additional staff member in such a conference.

Where a member of staff needs to complete a statutory SEND Annual Review or a GRIP Review, these may be done by phone call or via video conferencing or a meeting in school. The member of staff conducting these reviews must follow all published safeguarding guidance from Derbyshire County Council and the government when in a voice call or a video conference. Additionally, in a video conference staff must ensure that they think carefully about their background and should preferably blur the background or use a wall/area of their home that does not give away details about their home or location and there must be no family members or pets visible. The staff member must also use professional language as appropriate.

If IT staff are unavailable to offer support, our contingency plan is to contact a member of SLT who will then forward your query to someone who can help.

Below is additional advice for school staff on how to stay safe online and when using technology and social media:

- review your privacy settings, and ensure that they are sufficiently robust.
- sites such as Facebook allow you to view your page as different groups of people, e.g. friends, non-friends.
- privacy tools that are available on many social media sites include: customising who can see your posts; controlling who can contact you and make 'friend' requests; keeping your location private; and approving tags before they are published.
- discuss expectations around tagging posts with friends and family. For instance, you may prefer to not be tagged in any posts on social media.
- regularly search your name in search engines and social media sites to check what information there is on the internet about you. It is standard practice for employers to search prospective employees online, so search yourself online when applying for any posts. When searching, check variations of your name and even nicknames.
- if offensive or hurtful information is posted about you online, for instance, by a student or parent, never retaliate to the message. Make copies of all offensive content, including screenshots and URLs, and pass them on to the Headteacher. If offensive material has been posted about you online, you can use the reporting procedures of the site involved to get the material taken down.
- only use work equipment and email for work uses – and do not let anyone else, including colleagues and family members, use them.
- ensure all of your devices, including work ones, are password protected. Do not give your password to anyone else and do not leave your screen unlocked if you move away from the device.
- do not befriend any current students on social media. If students are consistently attempting to 'friend' you on social media, report this to the Headteacher.
- very carefully consider the implications of befriending former students on social media, especially as they may have friends, siblings or connections to current students. Similarly, there are potential implications of befriending parents of students on social media – even if they are also a colleague. Therefore, it is recommended that staff do not friend former students or parents on social media. If you do decide to do this, let the Headteacher know.
- keep your personal phone number, email address, social media accounts and online chat or video conferencing services accounts private and do not share with students or parents.
- when using social media, before posting or commenting on items, consider whether you would be happy for your employer, colleagues, students and parents to see it. If you wouldn't want them to, then don't post it online.
- never criticise the school, employer, students or parents online.

The school will consider the safeguards around loaning equipment and will take advice from the school IT Support Team on the issues.

The school will work with any further guidance issued by the Local Authority in respect to remote working and learning, and when using online means to communicate with children and their families.

Staff will continue to be alert to signs that a child may be at risk of harm online, and act on any concerns immediately, following our reporting procedures as set out in section.

The school will ensure children know how to report any concerns they have back to the school, and signpost them to other sources of support if required.

Working with Parents and Carers

The school will ensure parents and carers:

- are aware of the potential risks to children online and the importance of staying safe online.
- are aware of what the school is asking children to do online, including what sites they will be using and who they will be interacting with from our school. Are aware that parents/carers should only use reputable online companies or tutors if they wish to supplement the remote teaching and resources the school provides.
- know additional resources that are available for support to keep their children safe online. The school has dedicated a section of the website to advice and guidance for parents/carers and students in relation to online safety. This is updated as additional helpful resources become available.

Access to pre-recorded lessons should only be made available via the school's access to Google Classroom. Video/audio conferencing may only be performed using Google Meet.

Use of digital and video images

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

The school will inform and educate users about these risks and implement policies to reduce the likelihood of the potential for harm:

- when using digital images, staff should inform and educate students 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 are published on the school website / social media / local press
- in accordance with guidance from the Information Commissioner's Office, parents / carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use in not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published / made publicly available on social networking sites, nor should parents / carers comment on any activities involving other students 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 students are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.

- students must not take, use, share, publish or distribute images of others without their permission
- photographs published on the website, or elsewhere that include students will be selected carefully and will comply with good practice guidance on the use of such images.
- students' full names will not be used anywhere on a website or blog, particularly in association with photographs.
- student's work can only be published with the permission of the student 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:

- has a Data Protection Policy.
- implements the data protection principles and can demonstrate that it does so
- has paid the appropriate fee to the Information Commissioner's Office (ICO).
- has appointed a Data Protection Officer (DPO) who has effective understanding of data protection law and is free from any conflict of interest
- has a "Record of Processing Activities" in place and knows exactly what personal data is held, where, why and which member of staff has responsibility for managing it.
- the Record of Processing Activities lists the lawful basis for processing personal data (including relevant consent). Where special category data is processed, and additional lawful basis is listed
- has an "information asset register" in place and knows exactly what personal data is held, where, why and which member of staff has responsibility for managing it
- information asset register lists the lawful basis for processing personal (including, where relevant, consent). Where special category data is processed, and additional lawful basis will have also been listed
- will hold 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 "retention schedule" supports this.
- data held is accurate and up to date and held only for the purpose it was held for. Systems are in place to identify inaccuracies, such as parents to check emergency contact details at suitable intervals
- provides staff, parents, volunteers, teenagers and older children with information about how the school looks after their data and what their rights are in a clear Privacy Notice
- has procedures in place to deal with the individual rights of a data subject, e.g., one of the dozen rights applicable is that Subject Access which enables an individual to see/have a copy of the personal data held about them
- carries out Data Protection Impact Assessments (DPIA) where necessary e.g. to ensure protection of personal data when accessed using remote access solutions, or entering into a relationship with a new supplier
- has undertaken appropriate due diligence and has data protection compliant contracts in place with any data processors
- there are clear and understood data retention policies and routines for the deletion and disposal of data.
- reports any relevant breaches to the Information Commissioner within 72 hours of becoming aware of the breach as required by 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
- has Freedom of Information Policy which sets out how it will deal with FOI requests.

- provides data protection training for all staff 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.

Staff must ensure that they:

- at all times take care to ensure the safekeeping 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 school.
- can help data subjects understand their rights and know how to handle a request whether verbal or written and know who to pass it to in the school
- only use encrypted data storage for personal data
- will not transfer any school personal data to personal devices
- use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data.
- transfer data using encryption, a secure email account (where appropriate), and secure password protected devices

When personal data is stored on any portable computer system, memory stick or any other removable media:

- the data must be encrypted and password protected.
- the device must be password protected. (many memory sticks / cards and other mobile devices cannot be password protected)
- the device must offer approved virus and malware checking software.
- the data must be securely deleted from the device, in line with school policy once it has been transferred or its use is complete.

Communications

A wide range of rapidly developing communications technologies has the potential to enhance learning. When using communication technologies the school considers the following as good practice:

- the official school email service may be regarded as safe and secure and is monitored. Users should be aware that email communications are monitored. Staff and students should therefore use only the school email service to communicate with others when in school, or on school systems (e.g. by remote access/Google Drive/Google Classroom).
- users must immediately report, to the IT Network Manager, the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.
- any digital communication between staff and students or parents / carers (email, social media, chat, blogs, Virtual Learning Environment (VLE), remote on-line learning 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 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 have a duty of care to provide a safe learning environment for students and staff. Schools 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 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 students, 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 students, parents / carers or school staff
- they do not engage in online discussion on personal matters relating to members of the school community
- personal opinions should not be attributed to the school
- security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information

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
- 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 account. 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.
- 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

The school's use of social media for professional purposes will be checked regularly by the Online Safety Coordinator to ensure compliance with the school policies.

Dealing with unsuitable / inappropriate activities

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

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

User Actions		
Users shall not access online content (including apps, games, websites) to make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:		
	Unacceptable	**Unacceptable and illegal**
Child sexual abuse imagery –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**
Hate crime		**X**
Incitement to and threats of violence		**X**
Public order offences – harassment and stalking		**X**
Offences relating to sexual images, i.e., revenge and extreme pornography		**X**
Weapons/firearms' offences		**X**
Drug related offences		**X**
Fraud and financial crime including money laundering		**X**
threatening behaviour, including promotion of physical violence or mental harm (Public Order Act)		**X**
Promotion of extremism or terrorism		**X**

Users shall not undertake activities that are not illegal but are classified as unacceptable in the school set of policies:		
	Unacceptable	**Unacceptable and illegal**
Promotion of any kind of discrimination	**X**	
Any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute	**X**	
Using school systems to run a private business	**X**	
Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school	**X**	
Infringing copyright (Could infringe copyright law but not always illegal)	**X**	
Revealing or publicising confidential or proprietary information (e.g. financial / personal information, databases, computer / network access codes and passwords)	**X**	
Creating or propagating computer viruses or other harmful files (Illegal if you spread them), Computer Misuse act 1990)	**X**	
Accessing inappropriate material/activities online in a school setting including pornography, gambling, drugs (informed by the school's acceptable use policy filtering practices)	**X**	

Responding to incidents of misuse

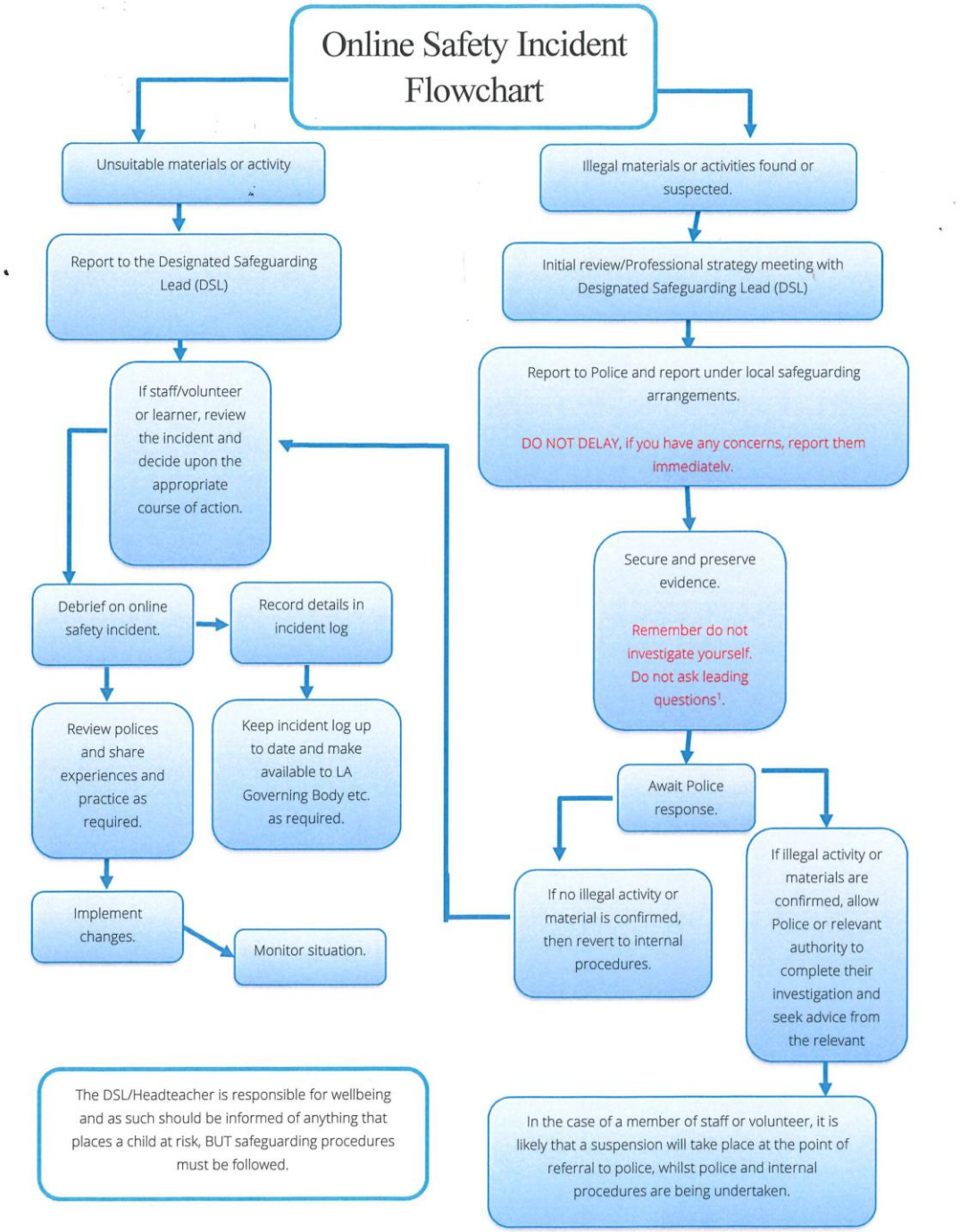
This guidance is intended for use when staff need to manage incidents that involve the use of online services. It encourages a safe and secure approach to the management of the incident. Incidents might involve illegal or inappropriate activities (see "User Actions" above).

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, complains and managing allegations policies.
- all members of the school community will be made aware of the need to report online safety incidents
- reports will be dealt with as soon as is practically possible once they are received
- the DSL, Online Safety Coordinator and other responsible staff have appropriate skills and training to deal with online safety risks

Illegal Incidents

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



Other Incidents

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

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

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

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

School Actions & Sanctions

It is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the school community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal behaviour / disciplinary procedures by follow up from the safeguarding team.