“Let your light shine brightly.”

Matthew 5:16

Online Safety Policy

Policy accepted by SLT on:	20/9/2021
Next review:	Autumn 2023
Signed (Headteacher):	R. Kaye
Statutory policy: Yes/No	**On school website:** Yes/No

ONLINE SAFETY POLICY

This policy is based on Somerset's *Model School Online Safety Policy* (eLIM, Sept 2020). It has been written in line with *Keeping children safe in education* (DfE, Sept 2021) (*KCSIE 2021*), *Teaching online safety in schools* (DfE, June 2019) and other statutory documents.

1. Scope of policy

This policy applies to all members of the school community, including staff, pupils, volunteers, parents/carers, visitors and community users.

The Education and Inspections Act 2006 empowers Headteachers, to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour.

This policy is pertinent to incidents such as cyberbullying and inappropriate use of social networking by pupils and staff, which may take place out of school, but are linked to membership of the school.

This policy also applies to both staff and pupil use of technology for remote/online learning as part of a blended approach and during any school closures (partial or full), e.g. the use of Teams to communicate and educate during a national/local lockdown or due to severe weather.

KCSIE 2021 sets out specific responsibilities for governing bodies to ensure:

- children are taught about online safety;
- appropriate filters and appropriate monitoring systems are in place;
- online safety training for staff is integrated, aligned and considered as part of the overarching safeguarding approach.

The school will manage online safety as described within this policy and associated behaviour and anti-bullying policies, and will inform parents and carers of known incidents of inappropriate online safety behaviour that take place in and out of school.

This Online Safety Policy should be read in conjunction with the following other linked school policies:

- Acceptable Use Policy
- Anti-Bullying Policy
- Child Protection and Safeguarding Policy
- Data Protection and Information Security Policy (Incorporating reference to GDPR)
- Relationship and Behaviour Policy.

2. Schedule for development, monitoring and review

The implementation of the Online Safety Policy will be monitored three times each year by the Headteacher and School Business Manager, reporting to the Full Governing Body annually. Monitoring will include:

- the log of reported incidents;
- the Internet monitoring log;
- surveys or questionnaires of learners, staff, parents and carers;
- other documents and resources;
- future developments.

This Online Safety Policy will be reviewed annually and will be under continuous revision in response to significant new developments in the use of technologies, new threats to online safety or incidents that have taken place.

3. Roles and responsibilities

The Headteacher and Governors oversee the safe use of technology when children and learners are in their care and act immediately if they are concerned about bullying, radicalisation or other aspects of children's well-being. They are responsible for ensuring the safety (including online and the prevention of being drawn into terrorism) of all members of the school community. They have concern for the online reputation of the school.

KCSIE 2021 Appendix C states: "the designated safeguarding lead should take lead responsibility for safeguarding and child protection (including online safety)".

At Christ Church, the Headteacher/Designated Safeguarding Lead (DSL) is also the Data Protection Officer and Online Safety Lead.

The Online Safety Lead must have an overview of the serious child protection issues that arise from sharing of personal data, access to illegal or inappropriate materials (including extremism and radicalisation, inappropriate online contact with adults, potential or actual incidents of grooming and cyberbullying.)

The Online Safety Lead will meet with the School Business Manager and Online Safety Link Governor three times a year to implement and monitor the Online Safety Policy and Acceptable Use Policy.

Governors

- Approve the Online Safety Policy.
- Monitor the effectiveness of the Online Safety Policy.
- Delegate a governor to act as Online Safety Link.

- Online Safety Link Governor reports to governors to verify that the filtering, monitoring and or supervision systems are in place to identify children accessing or trying to access harmful and inappropriate content online.

Senior Leaders

- Ensure that all staff receive suitable CPD to carry out their online safety roles, including online risks of extremism and radicalisation.
- Create a culture where staff and learners feel able to report incidents.
- Ensure that there is a progressive online safety curriculum in place.
- Ensure that there is a system in place for monitoring online safety.
- Follow correct procedure in the event of a serious online safety allegation being made against a member of staff or pupil.
- Inform the local authority (LA) about any serious online safety issues.
- Ensure that the school infrastructure/network is as safe and secure as possible.
- Ensure that policies and procedures approved within this policy are implemented.
- Use an audit to annually review online safety with the school's technical support.
- Work with the Online Safety Lead/ DSL/Data Protection Officer to ensure that the Remote/Online Learning Strategy developed and implemented by the school meets safeguarding and online safety requirements.

Online Safety Lead

- Log, manage and inform others of online safety incidents and how they have been resolved where this is appropriate.
- Lead the establishment and review of online safety policies and documents.
- Work with the Subject Leaders for Personal, Social, Health and Citizenship Education (PSHCE), Relationships and Sex Education (RSE) and Computing/ICT to embed and monitor a progressive online safety curriculum for pupils, as part of both RSE and Computing.
- Ensure that the school's Remote/Online Learning Strategy developed and implemented by the school meets safeguarding and online safety requirements.
- Ensure all staff are aware of the procedures relating to online safety.
- Provide and/or broker training and advice for staff.
- Attend updates, subscribe to appropriate newsletters and liaise with Somerset County Council online safety staff and technical staff.
- Meet with Senior Leadership Team (SLT) and Online Safety Link Governor to regularly discuss incidents and developments.

All teaching and support staff

- Participate in any training and awareness-raising sessions.
- Read, understand, sign and act in accordance with the Online Safety Policy and Acceptable Use Policy.

- .
- Report any suspected misuse or concerns (within or outside school) to the Online Safety Lead/DSL and check this has been recorded and actioned.
- Provide appropriate online safety learning opportunities as part of a progressive online safety curriculum.
- Model the safe, positive and purposeful use of technology.
- Monitor the use of technology in lessons, extracurricular and extended school activities, including Online/Remote Learning.
- Be mindful of the additional safeguarding considerations required if delivering Online/Remote Learning.
- Demonstrate consistently high standards of personal and professional conduct, especially in relation to use of social networks, making sure that these are in line with school ethos and policies, including at the time of a critical incident.

Subject Leaders for PSHCE and RSE

- Work with the Online Safety Lead and Subject Leader for Computing/ICT to embed and monitor a progressive online safety curriculum for pupils.

Subject Leader for Computing/ICT

- Work with the Online Safety Lead and Subject Leaders for PSHCE and RSE to embed and monitor a progressive online safety curriculum for pupils.

Pupils

- Report concerns for themselves or others.
- Make informed and positive choices when using technology in school and outside school, considering the effect on themselves and others.

Parents and carers

- Discuss appropriate, healthy, safe use of technology and online safety issues with their child(ren) and monitor their home use of technology (including tablets, mobile phones and games devices) and the Internet.
- Keep up to date with issues through newsletters and other opportunities.
- Inform teacher/Headteacher of any online safety concerns.
- Use formal channels to raise matters of concern about their child(ren)'s education.
- Maintain responsible standards when referring to the school on social media.

Technical support provider

- Ensure the school's ICT infrastructure is as secure as possible and is protected from misuse or malicious attack.
- Ensure users may only access the school network using an approved password.
- Support the school to ensure that platforms selected by the school for Online/Remote Learning meet safeguarding and online safety requirements.

- Maintain and inform the SLT of issues relating to filtering.
- Keep up to date with online safety technical information and update others as relevant.
- Ensure use of the network is regularly monitored in order that any misuse can be reported to the Online Safety Lead for investigation.
- Ensure monitoring systems are implemented and updated.
- Ensure all security updates are applied (including anti-virus and Windows).

Community users

- Must agree to follow the Online Safety Policy and Acceptable Use Policy *before* being provided with access to school systems.
- Must demonstrate appropriate standards of personal and professional conduct in line with the Online Safety Policy and Acceptable Use Policy.

Education of pupils

A progressive planned online safety education programme takes place in line with *Teaching online safety in schools*, through discrete lessons and across the curriculum, for all children in all years, and is regularly revisited. Breadth and progression is ensured through reference to UKCIS's *Education for a Connected World* framework and is implemented through the use of Somerset ActiveBYTES scheme.

Within this:

- key online safety messages are reinforced through assemblies, Safer Internet Week (February), Anti-Bullying Week (November) and throughout all teaching;
- pupils are taught to keep themselves safe online and to be responsible in their use of different technologies as detailed in the Somerset ActiveBYTES scheme of work;
- pupils are guided to use age-appropriate search engines for research activities. Staff are vigilant in monitoring the content of the websites visited and encourage pupils to use specific search terms to reduce the likelihood of coming across unsuitable material;
- in lessons where Internet use is pre-planned and where it is reasonable, pupils are guided to sites checked as suitable for their use and processes are in place for dealing with any unsuitable material that is found in Internet searches;
- pupils are taught to be critically aware of the content they access online, including recognition of bias and extreme or commercial content. They are guided to validate the accuracy and reliability of information;
- pupils are taught to acknowledge the source of information used and to respect copyright when using material accessed on the Internet;
- the Online Safety Lead maintains and passes on knowledge of current concerns to be included within learning experiences;
- pupils are provided with opportunities to influence the online safety curriculum;

- pupils are educated to recognise and respond appropriately to “different forms of bullying, including cyberbullying” and given opportunities to support each other;
- a continuous provision map is used with the youngest learners and SEN learners to establish appropriate habits for responsible use of technology.

4. Education and information for parents and carers

Parents and carers will be informed about the ways the Internet and technology is used in school. They have a critical role to play in supporting their children with managing online safety risks at home, reinforcing key messages about online safety and regulating their home experiences. The school supports parents and carers to do this by:

- providing clear guidance about online safety expectations in and out of school;
- providing regular newsletter items and appropriate support materials;
- raising awareness through activities planned by pupils and staff;
- inviting parents to attend activities such as Online Safety Week, online safety assemblies or other meetings as appropriate;
- providing and maintaining links to up-to-date information on the school website.

5. Education of wider school community

The school provides information about online safety to organisations using school facilities, local play groups and nurseries, and members of the wider community, which where appropriate includes:

- details about the Online Compass review tool;
- online safety messages targeted to grandparents and other relatives.

6. Training of staff and governors

There is a planned programme of online safety training as part of the overarching safeguarding approach, in line with *KCSIE 2021*, for all staff and governors to ensure they understand their responsibilities, as outlined in the Online Safety Policy and Acceptable Use Policy. This includes:

- all staff knowing the DSL and the Online Safety Lead and their responsibilities;
- an annual audit of the online safety training needs of **all** staff;
- **all** new staff and governors receiving online safety training as part of their induction programme (NQTs will be supported to complete the UKCIS Online Safety Audit Tool);
- providing information to supply and student teachers on the school’s online safety procedures;
- the Online Safety Lead receiving regular updates through attendance at training sessions and reviewing regular online safety newsletters from the LA;
- this Online Safety Policy and its updates being shared and discussed in staff meetings and in governor meetings;
- the Online Safety Lead providing training within safeguarding training and as specific online safety updates and reviews;

- the Online Safety Lead providing guidance as required to individuals and seeking LA support on issues;
- staff and governors are made aware of the Professionals Online Safety Helpline (POSH) (0344 381 4772).

7. Peer-on-peer abuse

All members of staff are made aware that children can abuse other children (often referred to as peer-on-peer abuse). Children are encouraged to talk to members of staff if they feel they are the victim or perpetrator, or if they are aware of peer-on-peer abuse. This abuse may include the following.

8. Cyberbullying

Cyberbullying (along with all other forms of bullying) of any member of the school community will not be tolerated. Full details are set out in the school's policy on anti-bullying and behaviour. The school will follow procedures in place to support anyone in the school community affected by cyberbullying.

- Pupils and staff are made aware of a range of ways of reporting concerns about online bullying. This may be by telling a trusted adult, Online Bully Box, Childline App and phone number (0800 1111), POSH helpline (0344 381 4772).
- Pupils, staff, parents and carers are informed of their responsibilities to report any incidents of online bullying and advised to keep electronic evidence.
- All incidents of online bullying reported to the school will be recorded and action taken by the school.
- The school will follow procedures to investigate incidents or allegations of online bullying.
- The school will take steps where possible and appropriate, to identify the bully. This may include examining school system logs, identifying and interviewing possible witnesses, and contacting the service provider and the police.
- Pupils, staff, parents and carers will be required to work with the school to support the approach to online bullying and the school's online safety ethos.
- Sanctions for those involved in online bullying will follow those for other bullying incidents as indicated in the school's Relationship and Behaviour Policy and may include:
  - the bully being asked to remove any material deemed to be inappropriate or the service provider being contacted to remove content if the bully refuses or is unable to delete content;
  - Internet access being suspended at the school for a period of time;
  - the parent and carers of pupils being informed;
  - the police being contacted if a criminal offence is suspected.

9. Sexting

The school will follow UKCIS advice on how to respond to any incident of sexting. We will provide appropriate support for sexting incidents which take place in and out of school. Within school, any device which has an illegal image of a child under 18, or is suspected of having such an image, will be secured and switched off. This will then be reported to the DSL. An individual member of staff will not investigate, delete or pass on the image. The DSL will record any incident of sexting and the actions taken in line with advice from Somerset County Council.

10. Sexual harassment, including upskirting

All staff are made aware that sexual harassment can occur between two children of any age and sex, and can include online harassment. Online sexual harassment may be standalone, or part of a wider pattern of (sexual) harassment and/or violence and can include:

- non-consensual sharing of sexual images and videos;
- sexualised online bullying;
- unwanted sexual comments and messages, including on social media;
- sexual exploitation;
- coercion and threats;
- upskirting.

All staff are made aware of what upskirting is, and that it is illegal. Any incident of sexual harassment will be taken seriously and reported to the DSL. The DSL will record the incident(s) and the actions taken in line with DfE guidance and advice from Somerset County Council and/or the Police as necessary.

11. Prevent

The school works to ensure children are safe from terrorist and extremist material when accessing the Internet on the premises. Appropriate levels of filtering are in place through a managed filtering service which includes terms related to terrorism. Appropriate monitoring of Internet use will identify attempts to access such material. Children are educated to evaluate information accessed with a reporting procedure that identifies inappropriate sites so that action, including blocking, can be put into place.

Technical Infrastructure

The school ensures, when working with our technical support provider that the following guidelines are adhered to:

- The school ICT systems are managed in ways that ensure that the school meets online safety technical requirements.
- There are regular reviews and audits of the safety and security of school ICT systems.

- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, workstations and other devices from accidental or malicious attempts which might threaten the security of school systems and data with regard to:
  - ensuring ongoing backups take place and, in case of an incident, the school can restore data in line with our business continuity plan;
  - the downloading of executable files by users;
  - the extent of personal use that users (staff/pupils/community users) and their family members are allowed on laptops and other portable devices used out of school;
  - the installing of programs on school devices unless permission is given by the technical support provider or Computing/ICT coordinator;
  - the use of removable media (e.g. memory sticks) by users on school devices (see School Personal Data Policy for further detail);
  - the installation of up-to-date anti-virus software.
- Access to the school network and Internet will be controlled with regard to:
  - users having clearly defined access rights to school ICT systems through group policies;
  - users being provided with an appropriate username and password (considering accessibility of users with particular needs where supervision is put in place to monitor activity);
  - staff users being made aware that they are responsible for the security of their username and password, which they are required to change every 60 days (they must not allow other users to access the systems using their log on details);
  - the master/administrator passwords for all systems are available to the Headteacher and kept securely in an agreed place;
  - users immediately reporting any suspicion or evidence that there has been a breach of security;
  - an agreed process being in place for the provision of temporary access of “guests” (e.g. trainee or supply teachers, visitors) onto the school system (anyone allowed unsupervised access must be made aware of the Online Safety Policy and Acceptable Use Policy).
- The Internet feed will be controlled with regard to:
  - the school’s responsibility to “ensure appropriate filters and appropriate monitoring systems are in place” (*KCSIE 2021*);
  - Foundation Stage and Key Stage 1 pupils’ access will be supervised with access to specific and approved online materials;
  - Key Stage 2 pupils’ will be supervised (pupils will use age-appropriate search engines and online tools and activities);
  - requests from staff for sites to be removed from the filtered list being approved by the SLT and logged;
  - user-based filtering used to provide differentiated access for staff and pupils;
  - filtering issues being reported immediately.

- The IT System of the school will be monitored with regard to:
  - the school IT technical support regularly monitoring and recording the activity of users on the school IT systems;
  - online safety incidents being documented and reported immediately to the Online Safety Lead or DSL, who will arrange for these to be dealt with immediately in accordance with school policies.

12. Data Protection

The school's Data Protection Policy provides full details of the requirements that are required to be met in relation to Data Protection regulations. The school will:

- at all times take care to ensure the safe keeping of personal and sensitive data, minimising the risk of its loss or misuse, which must include regular back-ups and anti-virus protection updates;
- use personal data only on secure password-protected computers and other devices;
- ensure that users are properly "logged-off" at the end of any session in which they are accessing personal data;
- provide staff with secure equipment/services to store or transfer data, e.g. remote access, One Drive, SharePoint school portal, encryption and secure password-protected devices;
- remove data in line with the school's Data Retention Policy;
- ensure that all staff are aware of the need to immediately report any loss of personal or sensitive data to the Data Protection Lead and that relevant staff understand the full requirements of the Data Protection Act 2018;
- complete a privacy impact assessment and check the terms and conditions of sites/apps used for learning purposes to ensure that any pupil personal data is being held securely.

13. Use of digital images and sound

Photographs, video and sound recorded within school are used to support learning experiences across the curriculum, to share learning with parents and carers on our school's learning platform, and to provide information about the school on the website.

The school will:

- build a culture where permission is always sought before a photo is taken or video and sound are recorded, including encouraging pupils to seek permission from other pupils to take, use, share, publish or distribute images and sound;
- ensure verifiable permission from parents or carers is obtained before images, sound recordings or videos of pupils are electronically published on the school website, on social media or in the local press. The written consent, where pupils' images, video and sound are used for publicity purposes, is kept until the data is no longer in use;

- when using digital images, staff educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images, including on social networking sites;
- allow staff to take images, record video and sound to support educational aims, following the school policy regarding the sharing, distribution and publication of those. School equipment only is used. Personal equipment of staff is not allowed for this purpose;
- make sure that images, sound or videos that include pupils will be selected carefully with their knowledge, taking care 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;
- make adults and children aware of the risk that any published image, video and sound could be harvested, reused and repurposed;
- ensure that pupils' full names will not be used anywhere on the school website, school blogs or within school-branded social media, particularly in association with photographs;
- not publish pupils' work without their permission and the permission of their parents or carers;
- only hold digital/video images on school-approved secure storage areas. There is an expectation that images and recordings are not retained longer than necessary and in line with the school's Data Retention Policy;
- in accordance with guidance from the Information Commissioner's Office, parents/carers may be permitted to take videos and digital images or sound recordings of their children at/after school events for their own personal use. It is made clear that, to respect everyone's privacy and in some cases protection, these are not to 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 or in the sound recording. We ask parents/carers not to take digital/video images or record sound during an event if it is felt that it would spoil the experience for others. A statement is made before an event as to the expectations of the school;
- make clear to professional photographers who are engaged to record any events or provide a service that they must work according to the terms of the school's Online Safety Policy and will sign an agreement which ensures compliance with the Data Protection regulations and that images will only be used for a specific purpose, subject to parental consent. Photographers will not have unsupervised access to children and young people;

14. Communication (including use of mobile devices and social media)

A wide range of communications technologies increases effective administration and has the potential to enhance learning. The school will:

- ensure that the school uses secure business systems for communication;

- ensure that personal information is not sent via unsecure systems;
- ensure that governors use secure systems;
- make users aware that communications will be monitored by the school;
- inform users what to do if they receive online communication that makes them feel uncomfortable, is offensive, threatening or bullying in nature;
- teach pupils about email and other communication tools alongside safe, healthy appropriate use of technology and online safety issues through the scheme of work;
- only publish official staff email addresses where this is required;
- protect the identities of multiple recipients by using Bcc in emails;
- develop a strategic approach to Blended Learning which enables online/remote learning opportunities to make use of age-appropriate educationally focused sites that will be moderated by the school;
- when selecting online learning platforms, first consider data protection. Complete a privacy impact assessment and check the terms and conditions of sites/apps used for learning purposes to ensure that any pupil personal data is being held securely;
- provide staff with the tools to risk assess sites before use and check the sites' terms and conditions to ensure (a) the site is age appropriate and (b) whether content can be shared by the site or others without additional consent being given;
- make sure that access to platforms will be password protected and run with approval from the SLT;
- ensure that any digital communication between staff and pupils or parents and carers is open, transparent and professional in tone and content;
- control access to social media and social networking sites in school;
- have a process to support staff who wish to use social media in the classroom to safely set up and run a class blog/Twitter/YouTube account to share learning experiences;
- make sure that staff official blogs or wikis will be password protected and run with approval from the SLT;
- discuss with staff the personal use of email, online learning platforms, social networking, social media and personal publishing sites as part of staff induction, building an understanding of safe and professional behaviour in line with DfE advice, being careful about subjects discussed online
- staff are advised that no reference should be made to pupils, parents/carers or school staff on their personal social networking accounts;
- support staff to deal with the consequences of hurtful or defamatory posts about them online;
- register concerns (e.g. recording in Online Safety Log) regarding pupils' inappropriate use of email, social networking, social media and personal publishing sites (in or out of school) and raise with their parents and carers, particularly when concerning pupils' underage use of sites;

- inform the staff that in the case of a critical incident they should not make any comment on social media without the permission of the SLT;
- inform staff that personal devices should only be used at break and lunchtimes in restricted areas when they are not in contact with pupils, unless they have the permission of the Headteacher (turned off at other times);
- ensure that all staff understand that the Online Safety Policy and Acceptable Use Policy apply to the use of their own portable/wearable device for school purposes;
- inform staff and visitors that they are not allowed to use personal devices to take photographs or video in school for any purpose without the express permission of SLT;
- check any use of a personal device for an education purpose (where permission has been given) only uses the school's Internet connection on the school site;
- remind all staff that personal devices should be pin-code or fingerprint protected and not discoverable by third parties;
- advise staff not to use their personal mobile phone to contact pupils, parents and carers;
- provide a mobile phone for activities that require them;
- challenge staff and visitors when there is suspected misuse of mobile phones or devices;
- when pupils are allowed personal devices in school, they are used in line with the school's policies and expectations, and pupils understand they can be asked to account for their use;
- use the right to collect and examine any pupil device that is suspected of containing offensive, abusive or illegal content or is suspected of causing issues on the school Internet connection.

The following table shows how the school considers the way these methods of communication should be used.

	Staff & other adults				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/wearable technology in school				✓				✓
Use of mobile phones/wearable technology in lessons				✓				✓
Use of mobile phones/wearable technology in social time				✓				✓
Taking photos on mobile phones or other camera devices				✓				✓
Use of personal devices, including wearable technology				✓				✓
Use of “always on” voice-activated technology				✓				✓
Use of personal email addresses in school, or on school network	✓							✓
Use of school email for personal emails		✓	✓				✓	
Use of chat facilities, forums and closed groups in apps		✓	✓				✓	
Use of messaging apps		✓	✓					✓
Use of social networking sites		✓	✓					✓
Use of blogs		✓	✓					✓
Use of Twitter		✓	✓					✓
Use of video broadcasting, e.g. YouTube		✓	✓				✓	
Use of live video streaming, e.g. Microsoft Teams, Zoom		✓	✓				✓	

15. Assessment of risk

Methods to identify, assess and minimise risks will be reviewed regularly. As technology advances, the school will examine and adjust the Online Safety Policy. Part of this consideration will include a risk assessment:

- looking at the educational benefit of the technology;
- considering whether the technology has access to inappropriate material.

The school provides appropriate filtering and monitoring as stated in this policy. However, due to the global and connected nature of Internet content, it is not possible to guarantee that access to unsuitable material will never occur via a school device.

All users need to be reminded that the use of computer systems, without permission or for inappropriate purposes, could constitute a criminal offence under the Computer Misuse Act 1990, and breaches will be reported to the Police.

16. Reporting and response to incidents

The school will follow Somerset County Council's incident flowchart to respond to illegal and inappropriate incidents. (This can be found at https://www.somerset.org.uk/sites/edtech/eSafety/Leading/Incident%20Flowchart%202020.pdf)

More than one member of staff (at least one should be a senior leader) will be involved in this process and the same designated computer will be used for the duration of any investigation. All sites and content checked will be recorded and screen shots, signed and dated, will be kept where this is appropriate.

Where content being reviewed is suspected or known to include images of child abuse, the investigation will be referred to the Police immediately and no further access will be made by the school to the material.

- All members of the school community will be informed about the procedure for reporting online safety concerns (such as breaches of filtering, online bullying, extremism, radicalisation, illegal content).
- Staff will record incidents in the appropriate concerns log. All reported incidents will be dealt with and actions recorded.
- The DSL will be informed of any online safety incidents involving child protection concerns, which will then be escalated in accordance with school procedures.
- The school will manage online safety incidents in accordance with the school's Relationship and Behaviour Policy where appropriate.
- The school will inform parents and carers of any incidents or concerns in accordance with school procedures.
- After any investigations are completed, the school will debrief, identify lessons learnt and implement any changes required.

- Where there is cause for concern or fear that illegal activity has taken place or is taking place, then the school will contact Somerset Children Safeguarding Team and escalate the concern to the Police.
- If the school is unsure how to proceed with any incidents of concern, then the incident may be escalated to the Education Safeguarding Service or Local Authority Designated Officer (LADO).

If an incident or concern needs to be passed beyond the school, then the concern will be escalated to the Education Safeguarding Service to communicate to other schools in Somerset.

Should serious online safety incidents take place, the following external persons and agencies should be informed:

- Education Safeguarding Service – *via Somerset Direct where a pupil is involved*;
- LADO – *via Somerset Direct where a member of staff is involved*.

The Police will be informed where users 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;
- promotion or conduct of illegal acts, under the child protection, obscenity, computer misuse and fraud legislation;
- adult material that potentially breaches the Obscene Publications Act in the UK;
- criminally racist or terrorist material, verbally abusive or threatening material, and information which is false and known or believed by the sender to be false.

17. Sanctions and disciplinary proceedings

Sanctions and disciplinary procedures may be taken where users visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to (unless this is part of an investigation):

- child sexual abuse images;
- grooming, incitement, arrangement or facilitation of sexual acts against children contrary to the Sexual Offences Act 2003;
- pornography, adult or mature content;
- promotion of any kind of discrimination, racial or religious hatred;
- personal gambling or betting;
- personal use of auction sites;
- any site engaging in or encouraging illegal activity, including radicalisation and terrorism;
- threatening behaviour, including promotion of physical violence or mental harm;

- 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;
- using school systems to run a private business;
- use systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school;
- uploading, downloading or transmitting commercial software or any copyrighted materials belonging to third parties, without the necessary licensing permissions;
- revealing or publicising confidential or proprietary information (e.g. financial or personal information, databases, computer or network access codes and passwords);
- creating or propagating computer viruses or other harmful files;
- carrying out sustained or instantaneous high-volume network traffic (downloading or uploading files) that causes network congestion and hinders others in their use of the Internet.

In addition, the following table indicates school policy on these uses of the Internet:

	Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable
Online gaming (educational)		✓	✓	
Online gaming (non-educational)				✓
Online gambling				✓
Online shopping/ commerce		✓	✓	
File sharing (using p2p networks)		✓	✓	

18. Sanctions (pupils)

The 2011 Education Act increased powers with regard to the searching for and of electronic devices and the deletion of data. These are applied through the school's Relationship and Behaviour Policy.

Incidents will have unique contexts and may need different levels of sanctions, especially in relation to their type and severity. Therefore, ticks may appear in more than one column.

Please note: the ticks in place are actions which may be relevant.

Incidents involving pupils	Refer to class teacher/tutor	Refer to Key Stage 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. detention/exclusion
Deliberately producing, accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable/ inappropriate activities)			✓	✓		✓	✓		✓
Unauthorised use of non-educational sites during lessons	✓	✓			✓				
Unauthorised use of mobile phone/wearable technology/ personal tablet	✓	✓	✓			✓			
Unauthorised use of social networking/instant messaging/personal email	✓	✓	✓		✓	✓			
Unauthorised downloading or uploading of files	✓	✓	✓			✓			
Allowing others to access school network by sharing username and passwords	✓	✓	✓		✓			✓	
Attempting to access or accessing the school network, using another pupil's account	✓	✓			✓			✓	

Attempting to access or accessing the school network, using the account of a member of staff		✓	✓		✓	✓	✓		
Corrupting or destroying the data of other users	✓	✓				✓	✓		
Sending an email, text, instant message, tweet or post that is regarded as offensive, harassment or of a bullying nature	✓	✓	✓			✓	✓		
Continued infringements of the above, following previous warnings or sanctions		✓	✓			✓	✓		✓
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school		✓	✓			✓	✓	✓	✓
Using proxy sites or other means to subvert the school's filtering system		✓	✓		✓	✓	✓		✓
Accidentally accessing offensive or pornographic material and failing to report the incident		✓	✓		✓	✓	✓		
Deliberately accessing or trying to access offensive, pornographic or extremist material		✓	✓	✓	✓	✓	✓	✓	✓
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act		✓	✓		✓	✓	✓	✓	✓

19. Sanctions (staff)

Schools should populate the grid below marking appropriate possible sanctions. Incidents will have unique contexts and may need different levels of sanctions, especially in relation to their type and severity. Therefore, marks may appear in more than one column.

Please note: the ticks in place are actions which <u>may</u> be relevant.

Incidents:	Refer to line manager	Refer to Headteacher	Refer to local authority/HR	Refer to LADO(L)/Police(P)	Refer to technical support staff for action re filtering etc.	Disciplinary action: Warning	Disciplinary action: Suspension	Disciplinary action: Other
Deliberately producing, accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable/inappropriate activities)	✓	✓	✓	**L, P**	✓	✓	✓	✓
Excessive or inappropriate personal use of the Internet /social networking sites/ instant messaging/ personal email	✓	✓	✓		✓	✓	✓	✓
Unauthorised downloading or uploading of files	✓	✓	✓		✓	✓	✓	✓
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	✓	✓	✓		✓	✓	✓	✓

Careless use of personal data, e.g. holding or transferring data in an insecure manner	✓	✓	✓		✓	✓	✓	✓
Deliberate actions to breach data protection or network security rules	✓	✓	✓	**P**	✓	✓	✓	✓
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software	✓	✓	✓	**P**	✓	✓	✓	✓
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature to staff	✓	✓	✓	**P**	✓	✓	✓	✓
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature to learners	✓	✓	✓	**L, P**	✓	✓	✓	✓
Breech of the school online safety policies in relation to communication with learners	✓	✓	✓	**L, P**	✓	✓	✓	✓
Using personal email/ social networking/instant messaging/text messaging to carry out digital communications with pupils	✓	✓	✓	**L, P**	✓	✓	✓	✓
Actions which could compromise the staff member's professional standing	✓	✓	✓	**L, P**	✓	✓	✓	✓

Actions which could bring the school into disrepute or breach the integrity of the ethos of the school	✓	✓	✓	**L, P**	✓	✓	✓	✓
Using proxy sites or other means to subvert the school's filtering system	✓	✓	✓		✓	✓	✓	✓
Accidentally accessing offensive or pornographic material and failing to report the incident	✓	✓	✓	**L**	✓	✓	✓	✓
Deliberately accessing or trying to access offensive or pornographic material, or material that seeks to radicalise	✓	✓	✓	**L, P**	✓	✓	✓	✓
Breaching copyright or licensing regulations	✓	✓	✓		✓	✓	✓	✓
Continued infringements of the above, following previous warnings or sanctions	✓	✓	✓	**L, P**	✓	✓	✓	✓