Online Safety Policy

Holy Trinity School

Policy last reviewed: March 2025

Next review due: March 2026

Member of staff responsible: Assistant Headteacher, Safeguarding and DSL

Governor's Committee: Full Governing Board

Vision Statement:	Our vision is to be a centre of excellence for learning, inspired by Christian values, where every person in our school community fulfils their potential.
Mission Statement:	Our mission is to be a deeply Christian inclusive community which values every individual as a child of God.
Values Statement:	The school aims to serve its community by providing an education of the highest quality within the context of Christian belief and practice. It encourages an understanding of the meaning and significance of faith and promotes Christian values through the experience it offers to all its students.

Dignity	Underpinning all that we do is the core belief in the ultimate worth of each person as a child of God – precious, valued and loved by God. Dignity comes from the knowledge of our ultimate worth as human beings.
Community	Having understood our value as individual human beings, we express this value through the quality of the relationships that we share with each other. Community, living well together, is of very great importance to us as a school, as is the place we each take in the wider community locally, nationally and internationally.
Wisdom	As a school we seek to foster confidence, delight and discipline in seeking wisdom, knowledge and truth. This is achieved through the nurturing of academic habits and skills, emotional intelligence, resilience and creativity across the breadth of the curriculum.
Hope	As we prepare our students for the future we look to open up horizons of hope and aspiration, encouraging our students to embrace these with confidence and sending them out to make a difference to the world in which they live.

Contents

Overview

Aims

This policy aims to promote a whole school approach to online safety by:

- Setting out expectations for all Holy Trinity CofE Secondary School community members towards online behaviour and use of digital technology (including when devices are offline)
- Helping safeguarding and senior leadership teams to have a better understanding and awareness of all elements of online safeguarding through effective collaboration and communication with technical colleagues within BCTEC (e.g. for filtering and monitoring), curriculum leads (e.g. RSHE and Computing)
- Helping all stakeholders to recognise that online/digital behaviour standards (including social media activity) must be upheld beyond the confines of the school gates and school day, regardless of device or platform, and that the same standards of behaviour apply online and offline.
- Facilitating the safe, responsible, respectful and positive use of technology to support teaching & learning, increase attainment and prepare children and young people for the risks and opportunities of today's and tomorrow's digital world.
- Helping school staff working with children to understand their roles and responsibilities to work safely and responsibly with technology and the online world:

Scope

This policy applies to all members of the Holy Trinity CofE Secondary School community (including teaching, supply and support staff, governors, volunteers, contractors, students/pupils, parents/carers, visitors and community users) who have access to our digital technology, networks and systems, whether on-site or remotely, and at any time, or who use technology in their school role.

Roles and responsibilities

This school is a community, and all members have a duty to behave respectfully online and offline, to use technology for teaching and learning and to prepare for life after school, and to immediately report any concerns or inappropriate behaviour, to protect staff, pupils, families and the reputation of the school. We learn together, make honest mistakes together and support each other in a world that is online and offline at the same time.

All members of the school community should **read the relevant section in APPENDIX A of this document** that describes individual roles and responsibilities. Please note there is one for All Staff which must be read even by those who have a named role in another section.

Education and curriculum

Despite the risks associated with being online, Holy Trinity CofE Secondary school recognises the opportunities and benefits of children being online. Technology is a fundamental part of our adult lives and so developing the competencies to understand and use it, are critical to children's later positive outcomes. The choice to use technology in school will always be driven by pedagogy and inclusion.

As well as teaching about the underpinning knowledge and behaviours that can help pupils navigate the online world safely and confidently regardless of the device, platform or app, Teaching Online Safety in Schools recommends embedding teaching about online safety and harms through a whole school approach and provides an understanding of these risks to help tailor teaching and support to the specific needs of pupils, including vulnerable pupils.

The teaching of online safety, features prominently in the below areas of curriculum delivery but all staff and students use technology every day and all staff will reinforce the messages delivered by these subjects:

- Relationships education, relationships and sex education (RSE) and health (also known as RSHE or PSHE)
- Computing

However, as stated previously, it is the role of ALL staff to identify opportunities to thread online safety through all school activities, both outside the classroom and within the curriculum, supporting faculty/subject/key stage leads, and making the most of unexpected learning opportunities as they arise.

Whenever overseeing the use of technology (devices, the internet, generative AI tools) in school or setting as homework tasks, all staff should encourage sensible use, monitor what students are doing and consider potential risks and the age appropriateness of tasks. This includes supporting them with search skills, reporting and accessing help, critical thinking (e.g. disinformation, misinformation and fake news), access to age-appropriate materials and signposting, and legal issues such as copyright and data law.

The curriculum model we follow is found here:

https://www.holytrinity.w-sussex.sch.uk/Curriculum/

Annual reviews of curriculum plans / schemes of work (including for SEND pupils) take place and are used as an opportunity to follow this framework more closely in its key areas. We communicate with parents and carers about how we support pupils with their online safety learning, including what their children are being asked to do online and the sites they will be asked to access by teacher choice through the Jamf Application tool. This will then be reset by the teacher at the end of the lesson.

Handling safeguarding concerns and incidents

It is vital that all staff recognise that online safety is a part of safeguarding and so concerns must be handled in the same way as any other safeguarding concern. School procedures for dealing with online safety will be mostly detailed in the following policies:

- KCSIE

- Safeguarding and Child Protection Policy
- Anti-Bullying Policy
- Behaviour Policy (including school sanctions)
- Acceptable Use Policies
- Data Protection Policy, agreements and other documentation (e.g. privacy statement and consent forms for data sharing, image use etc)

This school commits to take all reasonable precautions to safeguard pupils online but recognises that incidents will occur both inside school and outside school (and that those from outside school will continue to impact pupils when they come into school or during extended periods away from school). All members of the school are encouraged to report issues swiftly to allow us to deal with them quickly and sensitively.

Any suspected online risk should be reported to the designated safeguarding lead as soon as possible on the same day. The reporting member of staff will ensure that a record is made of the concern on CPOMs - this includes any concerns raised by the filtering and monitoring systems

Any concern/allegation about staff misuse is always (similar to any safeguarding concern) referred directly to the Executive Headteacher, unless the concern is about the Headteacher in which case the complaint is referred to the Chair of Governors and the LADO (Local Authority's Designated Officer). Staff may also use the NSPCC Whistleblowing Helpline.

We will inform parents/carers of online safety incidents involving their children, and the Police where staff or pupils engage in or are subject to behaviour which we consider is particularly concerning or breaks the law.

The school should ensure all online safety reporting procedures are sustainable for any unforeseen periods of closure.

Misuse of school technology (devices, systems, networks or platforms)

Holy Trinity CofE Secondary school will have clear and well communicated rules and procedures to govern pupil and adult use of school networks, connections, internet connectivity and devices, cloud platforms and social media (both when on school site and outside of school).

These are defined in the relevant Acceptable Use Policy (which can be found on the school website). Where pupils contravene these rules, the school behaviour policy will be applied; where staff contravene these rules, action will be taken as outlined in the staff code of conduct/handbook.

It will be necessary to reinforce these as usual at the beginning of any school year but also to remind pupils that the same applies for any home learning that may take place.

Further to these steps, the school reserves the right to withdraw – temporarily or permanently – any or all access to such technology, or the right to bring devices onto school property.

Acceptable use

The school has defined what it regards as acceptable/unacceptable use and this is shown in the tables below.

Acceptable use agreements

An Acceptable Use Agreement is a document that outlines a school's expectations on the responsible use of technology by its users. In most schools they are signed or acknowledged by their staff as part of their conditions of employment. Some may also require learners and parents/carers to sign them, though it is more important for these to be regularly promoted, understood and followed rather than just signed. There is a range of acceptable use agreements in the appendices.

In the tables in **Appendix B** it can be found which activities are deemed acceptable/unacceptable or illegal and separately which non educational activities are permitted for students and staff.

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

- when communicating in a professional capacity, staff should ensure that the technologies they use are officially sanctioned by the school.
- any digital communication between staff and learners or parents/carers (e-mail, social media, learning platform, etc.) must be professional in tone and content. *Personal e-mail addresses, text messaging or social media must not be used for these communications.*
- staff should be expected to follow good practice when using personal social media regarding their own professional reputation and that of the school and its community
- users should immediately report to a nominated person – in accordance with the school policy – the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.
- relevant policies and permissions should be followed when posting information online e.g., school website and social media. Only school e-mail addresses should be used to identify members of staff and learners.

Social media incidents

Social media incidents involving pupils are often safeguarding concerns and should be treated as such and staff should follow the safeguarding policy. Other policies that govern these types of incidents are the school's Acceptable Use Policies/online safety.

Breaches will be dealt with in line with the school behaviour policy (for pupils) or code of conduct/handbook (for staff). See the social media section later in this document for rules and expectations of behaviour for children and adults.

Further to this, where an incident relates to an inappropriate, upsetting, violent or abusive social media post by a member of the school community (e.g. parent or visitor), Holy Trinity School where possible will request that the post be deleted and will expect this to be actioned promptly.

Where an offending post has been made by a third party, the school may report it to the platform it is hosted on, and may contact the Professionals' Online Safety Helpline (POSH) (run by the UK Safer Internet Centre) for support or help to accelerate this process.

CCTV

CCTV is strategically placed around the school. It can be found in all corridors, locker areas, stairwells and large spaces such as the hall and sixth form centre as well as the perimeter of the main buildings, reception and the car park. CCTV is a deterrent for poor behaviour and in place to help students and staff feel safe.

CCTV will be used to follow up behaviour or safeguarding incidents between students. Senior Leadership and Pastoral staff have access to CCTV and can cut footage and store in school online files only. CCTV remains available for 2 weeks before it is deleted. All students are made aware of CCTV and the cameras are visible. Footage may be saved and provided to the Police using a NICE link if they are investigating an incident which occurred on site.

Extremism

The school has obligations relating to radicalisation and all forms of extremism under the Prevent Duty. Staff will not support or promote extremist organisations, messages or individuals, give them a voice or opportunity to visit the school, nor browse, download or send material that is considered offensive or of an extremist nature. We ask for parents' support in working with their child, especially relating to social media.

Data protection

All pupils, staff, governors, volunteers, contractors and parents are bound by the school's data protection. Data Protection at Holy Trinity CofE Secondary School is outsourced to Bulletproof.

Schools should remember that data protection does not prevent, or limit, the sharing of information for the purposes of keeping children safe. As outlined in *Data protection in schools*, 2023, "It's not usually necessary to ask for consent to share personal information for the purposes of safeguarding a child." And in KCSIE 2024, "The Data Protection Act 2018 and UK GDPR do not prevent the sharing of information for the purposes of keeping children safe. Fears about sharing information must not be allowed to stand in the way of the need to safeguard and promote the welfare and protect the safety of children."

Appropriate filtering and monitoring

The designated safeguarding lead (DSL) has lead responsibility for filtering and monitoring and works closely with the Safeguarding Managers, BCTEC leaders and Safeguarding admin team to implement the DfE filtering and monitoring standards, which require schools to:

- identify and assign roles and responsibilities to manage filtering and monitoring systems.
- review filtering and monitoring provision at least annually.
- block harmful and inappropriate content without unreasonably impacting teaching and learning.
- have effective monitoring strategies in place that meet their safeguarding needs.

We look to provide 'appropriate filtering and monitoring (as outlined in Keeping Children Safe in Education) at all times.

We ensure ALL STAFF are aware of filtering and monitoring systems and play their part in feeding back about areas of concern, potential for students to bypass systems and any potential over blocking. They can submit concerns at any point via the BCTEC Portal.

Technical and safeguarding colleagues work together closely to carry out reviews and check to ensure that the school responds to issues and integrates with the curriculum. The Head of School, Business Manager, DSL and BCTEC representative meet on a regular basis to review all current cases.

Safe Search is enforced on any accessible search engines on all devices. You can only use the search engines set up on the devices by BCTEC. You Tube is available for all staff to use. You Tube is disabled for all students but can be used if applicable to examination work.

Out of hours, our policies are:

- for filtering devices, all processes continue to happen outside of working hours

- for monitoring devices, the Safeguarding team receive a report every 24 hours during term time. This will be less frequent during holiday periods at a weekly basis. The DSL takes appropriate action on a case-by-case basis.

- There is an expectation that parents will also monitor any use of devices in their own homes, particularly during the weekend and holiday periods

Staff will be reminded of the systems in place and their responsibilities at induction and start of year safeguarding as well as via AUPs and regular training reminders in the light of the annual review and regular checks that will be carried out.

The DfE recommends the following standards which we require our staff to follow and engage with:

- Physically monitoring by staff watching screens of users. (All Staff)
- Live supervision by staff on a console with device management software such as Teacher JamF
- Network monitoring using log files of internet traffic and web access (DSL, Safeguarding Team)
- individual device monitoring through software or third-party services (BCTEC)

Messaging/commenting systems (incl. email, learning platforms & more)

<u>Authorised systems</u>

- Pupils at this school communicate with each other and with staff using school email and Microsoft TEAMS
- Staff at this school use the email system provided by Microsoft office for all school emails. They never use a personal/private email account (or other messaging platform) to communicate with children or parents, or to colleagues when relating to school/child data, using a non-school-administered system. Staff are permitted to use this email system to communicate with anyone associated with their work
- Staff at this school use Microsoft TEAMS to communicate with staff or students in their classes

Any systems above are centrally managed and administered by the school or authorised IT partner (i.e. they can be monitored/audited/viewed centrally; are not private or linked to private accounts). This is for the mutual protection and privacy of all staff, pupils and parents, supporting safeguarding best-practice, protecting children against abuse, staff against potential allegations and in line with UK data protection legislation.

Use of any new platform or app with communication facilities or any child login or storing school/child data must be approved in advance by the school and centrally managed.

Where devices have multiple accounts for the same app, mistakes can happen, such as an email being sent from, or data being uploaded to the wrong account. If this a private account is used for communication or to store data by mistake, the DSL/Headteacher/DPO (the particular circumstances of the incident will determine whose remit this is) should be informed immediately.

Behaviour / usage principles of messaging/commenting systems

- More detail for all the points below are given in the school's Acceptable Use Agreements, Behaviour Policy and Staff Code of Conduct.
- Appropriate behaviour is expected at all times, and the system should not be used to send inappropriate materials or language which is or could be construed as bullying, aggressive, rude, insulting, illegal or otherwise inappropriate, or which (for staff) might bring the school into disrepute or compromise the professionalism of staff.
- Data protection principles will be followed at all times when it comes to all school communications, in line with the school Data Protection Policy and only using the authorised systems mentioned above.
- Pupils and staff are allowed to use the email system for reasonable (not excessive, not during lessons) personal use but should be aware that all use is monitored, their emails may be read and the same rules of appropriate behaviour apply at all times. Emails using inappropriate language, images, malware or to adult sites may be blocked and not arrive at their intended destination (and will be dealt with according to the appropriate policy and procedure).

Use of generative AI

- At Holy Trinity Church of England School, we acknowledge that generative AI platforms (e.g. ChatGPT or Bard for text creation or the use of Co-Pilot or Adobe Firefly to create images and videos) are becoming widespread. We are aware of and follow the DFE's Guidance on this. In particular:
- We will talk about the use of these tools with pupils, staff and parents – their practical use as well as their ethical pros and cons. We promote the concept of Digital Wisdom.
- We are aware that there will be use of these apps and exposure to AI creations on devices at home for some students – these experiences may be both positive/creative and also negative (inappropriate data use, misinformation, bullying, deepfakes, undressing apps).
- The use of any generative AI in Exams, or to plagiarise and cheat is prohibited, and the Behaviour Policy will be used for any pupil found doing so.
- The school is currently working on producing an AI policy which covers this area in more depth

Online storage or learning platforms

All the principles outlined above also apply to any system to which you log in online to conduct school business, whether it is to simply store files or data (an online 'drive') or collaborate, learn and teach.

For all these, it is important to consider data protection and cyber security before adopting such a platform or service and at all times when using it. Any new platforms will be approved by the Head of School.

School website

The school website is a key public-facing information portal for the school community (both existing and prospective stakeholders) with a key reputational value. The Head of School and Governors have delegated the day-to-day responsibility of updating the content of the website and ensuring compliance with DfE stipulations to members of the admin team.

The website is managed by BCTEC with key members of staff including the Head of Schools PA having access to place key messages online when directed.

Where staff submit information for the website, they are asked to remember that schools have the same duty as any person or organisation to respect and uphold copyright law. Sources must always be credited, and material only used with permission. There are many open-access libraries of public-domain images/sounds etc that can be used. Finding something on Google or YouTube does not mean that copyright has been respected.

Digital images and video

When a pupil/student joins the school, parents/carers are asked if they give consent for their child's image to be captured in photographs or videos, for what purpose (beyond internal assessment, which does not require express consent) and for how long. Parents answer as follows:

Whenever a photo or video is taken/made, the member of staff taking it will check the latest database on the School Management Information System before using it for any purpose.

Any pupils shown in public facing materials are never identified with more than first name (and photo file names/tags do not include full names to avoid accidentally sharing them).

All staff are governed by their contract of employment and the school's Acceptable Use Policy, which covers the use of mobile phones/personal equipment for taking pictures of pupils, and where these are stored. At Holy Trinity, no member of staff will ever use their personal phone to capture photos or videos of pupils.

Staff, parents and students are reminded annually about the importance of not sharing images on social media or otherwise without permission, due to reasons of child protection (e.g. children who are looked after by the local authority may have restrictions in place for their own protection), data protection, religious or cultural reasons, or simply for reasons of personal privacy.

We encourage young people to think about their online reputation and digital footprint, so we should be good adult role models by not oversharing (or providing embarrassment in later life – and it is not for us to judge what is embarrassing or not).

Students are taught about how images can be manipulated in their online safety education programme and also taught to consider how to publish for a wide range of audiences which might include governors, parents or younger children.

Students are advised to be very careful about placing any personal photos on social media. They are taught to understand the need to maintain privacy settings so as not to make public, personal information.

Students are taught that they should not post images or videos of others without their permission. We teach them about the risks associated with providing information with images (including the name of the file), that reveals the identity of others and their location. We teach them about the need to keep their data secure and what to do if they / or a friend are subject to bullying or abuse.

All of the above is done through both the REACH and Computing curriculums, as well as pastoral assemblies and tutor times.

Device usage

AUPs remind those with access to school devices about rules on the misuse of school technology – devices used at home should be used just like if they were in full view of a teacher or colleague. Please read the following in conjunction with those AUPs and the sections of this document which impact upon device usage, e.g. copyright, data protection, social media, misuse of technology, and digital images and video.

Personal devices including wearable technology

Personal devices cannot be used during the school day and Sixth Formers can only use in the Common Room.

- **Students** – Students must follow the mobile phone policy. Please follow the link to read the full policy.
  https://www.holytrinity.w-sussex.sch.uk/docs/Policies/Mobile_Phone_Policy.pdf
- **All staff who work directly with children** should leave their mobile phones on silent and only use them in private staff areas during school hours.
- Student/staff data should never be downloaded onto a private phone. If a staff member is expecting an important personal call when teaching or otherwise on duty they must liaise with their line manager. Students who have a diagnosed medical condition, for example diabetes, where their phone is used to manage their condition will have permission to use their phone. Any other students wishing to use their personal phone must have sought and agreed permission with their Year team. **Volunteers, contractors, governors** should leave their phones in their pockets and turned off. Under no circumstances should they be used in the presence of children or to take photographs or videos. If this is required (e.g. for contractors to take photos of equipment or buildings), this should be done in the presence of a member staff.
- Parents are asked not to call pupils on their mobile phones during the school day; urgent messages can be passed via the school office.
- Students are not allowed to use a mobile hotspot to provide internet to their school device as this would potentially bypass filtering controls.

Use of school devices

Staff and pupils are expected to follow the terms of the school acceptable use policies for appropriate use and behaviour when on school devices, whether on site or at home.

School devices are not to be used in any way which contravenes AUPs, behaviour policy / staff code of conduct.

Wi-Fi is accessible to staff, students, contractors and visitors for school-related internet use limited personal use within the framework of the acceptable use policy. All such use is monitored.

School devices for staff or students are restricted to the apps/software installed by the school, whether for use at home or school, and may be used for learning and reasonable as well as appropriate personal use.

All and any usage of devices and/or systems and platforms may be tracked.

Trips / events away from school

For school trips/events away from school, trip leaders where possible will have a school phone and this number will be used for any authorised or emergency communications with staff and parents. Teachers may use their personal phone in an emergency and to communicate with staff on a trip. They will not use their phone to take pictures of students on the trip.

Searching and confiscation

In line with the DfE guidance 'Searching, screening and confiscation: advice for schools', the Executive Headteacher, Head of School and staff authorised by them have a statutory power to search pupils/property on school premises. This includes the content of mobile phones and other devices, for example as a result of a reasonable suspicion that a device contains illegal or undesirable material, including but not exclusive to sexual images, pornography, violence or bullying. Full details of the school's search procedures are available in the Behaviour Policy found on the school website.

Appendix A – Roles

Please read the relevant roles & responsibilities section from the following pages.

All school staff must read the "**All Staff**" section **as well as** any other relevant to specialist roles.

Roles:

- All Staff
- Head of School
- Designated Safeguarding Lead
- Governing Body, led by Safeguarding Link Governor
- REACH Leads
- Computing Lead
- Subject leaders
- Network Manager/technicians - BCTEC
- Data Protection Officer (DPO)
- Volunteers and contractors (including tutor)

- Pupils
- Parents/carers
- External groups including parent associations

All staff

All staff should sign and follow the staff acceptable use policy in conjunction with this policy, the school's main safeguarding policy, the code of conduct and school handbook and relevant parts of Keeping Children Safe in Education (KCSIE) to support a whole-school safeguarding approach.

They must report any concerns, no matter how small, to the designated safety lead as named in the AUP, maintaining an awareness of current online safety issues (see the start of this document for issues in 2024) and guidance (such as KCSIE), modelling safe, responsible and professional behaviours in their own use of technology at school and beyond and avoiding scaring, victim-blaming language.

Staff should also be aware of the DfE standards for filtering and monitoring and play their part in feeding back to the DSL about over blocking, gaps in provision or pupils bypassing protections. All staff are also responsible for the physical monitoring of pupils' online devices during any session/class they are working within.

Head of School

Key responsibilities:

- Foster a culture of safeguarding where online safety is fully integrated into whole-school safeguarding.
- Oversee and support the activities of the designated safeguarding lead team and ensure they work technical colleagues to complete an online safety audit in line with KCSIE (including technology in use in the school).
- Undertake training in offline and online safeguarding, in accordance with statutory guidance and Local Safeguarding Children Partnership support and guidance.
- Ensure ALL staff undergo safeguarding training (including online safety) at induction and with regular updates and that they agree and adhere to policies and procedures.
- Ensure ALL governors undergo safeguarding and child protection training and updates (including online safety) to provide strategic challenge and oversight into policy and practice and that governors are regularly updated on the nature and effectiveness of the school's arrangements
- Ensure the school implements and makes effective use of appropriate ICT systems and services including school-safe filtering and monitoring, protected email systems and that all technology including remote systems are implemented according to child-safety first principles.
- Better understand, review and drive the rationale behind decisions in filtering and monitoring as per the DfE standards—through regular liaison with technical colleagues and the DSL – in particular understand what is blocked or allowed for whom, when, and how as per KCSIE.
- Liaise with the designated safeguarding lead on all online safety issues which might arise and receive regular updates on school issues and broader policy and practice information.

- Support safeguarding leads and technical staff as they review protections for pupils in the home and remote-learning procedures, rules and safeguards
- Take overall responsibility for data management and information security ensuring the school's provision follows best practice in information handling; work with the DPO, DSL and governors to ensure a compliant framework for storing data but helping to ensure that child protection is always put first and data-protection processes support careful and legal sharing of information.
- Understand and make all staff aware of procedures to be followed in the event of a serious online safeguarding incident.
- Ensure suitable risk assessments are undertaken so the curriculum meets needs of pupils, including risk of children being radicalised.
- Ensure the school website meets statutory requirements

Designated Safeguarding Lead

Key responsibilities (remember the DSL can delegate certain online safety duties but not the overall responsibility; this assertion and all quotes below are from Keeping Children Safe in Education):

- The DSL should "take lead responsibility for safeguarding and child protection (including online safety and understanding the filtering and monitoring systems and processes in place).
- Ensure "An effective whole school approach to online safety as per KCSIE.
- Ensure the school is complying with the DfE's standards on Filtering and Monitoring.
- As part of this, DSLs will work with technical teams to carry out reviews and checks on filtering and monitoring, to compile the relevant documentation and ensure that safeguarding and technology work together. This will include a decision on relevant YouTube mode and preferred search engine/s etc.
- Where online safety duties are delegated and in areas of the curriculum where the DSL is not directly responsible, but which cover areas of online safety (e.g. RSHE), ensure there is regular review and open communication and that the DSL's clear overarching responsibility for online safety is not compromised or messaging to pupils confused.
- Ensure ALL staff and supply staff undergo safeguarding and child protection training (including online safety) at induction and that this is regularly updated.
    - This must include filtering and monitoring and help them to understand their roles.
    - All staff must read KCSIE Part 1.
    - Cascade knowledge of risks and opportunities throughout the organisation.
- Ensure that ALL governors and undergo safeguarding and child protection training (including online safety) at induction to enable them to provide strategic challenge and oversight into policy and practice and that this is regularly updated
- Take day-to-day responsibility for safeguarding issues and be aware of the potential for serious child protection concerns.
- Be mindful of using appropriate language and terminology around children when managing concerns, including avoiding victim-blaming language
- Remind staff of safeguarding considerations as part of a review of remote learning procedures and technology, including that the same principles of online safety and behaviour apply.
- Work closely with SLT, staff and technical colleagues to complete an online safety audit (including technology in use in the school)

- Work with the Head of School, DPO and Governors to ensure a compliant framework for storing data but helping to ensure that child protection is always put first, and data-protection processes support careful and legal sharing of information.
- Stay up to date with the latest trends in online safeguarding and "undertake Prevent awareness training.
- Receive regular updates about online safety issues and legislation, be aware of local and school trends.
- Ensure that online safety education is embedded across the curriculum in line with the statutory RSHE guidance.
- Promote an awareness of and commitment to online safety throughout the school community, with a strong focus on parents, including hard-to-reach parents
- Communicate regularly with SLT and the safeguarding governor/committee to discuss current issues (anonymised), review incident logs and filtering/change control logs and discuss how filtering and monitoring work and have been functioning/helping.
- Ensure all staff are aware of the procedures that need to be followed in the event of an online safety incident, and that these are logged in the same way as any other safeguarding incident.
- Ensure adequate provision for staff to flag issues when not in school and for pupils to disclose issues when off site
- Ensure staff follow a whole school approach and report all forms of child-on-child abuse.
- Pay particular attention to **online tutors**, both those engaged by the school as part of the DfE scheme who can be asked to sign the contractor AUP, and those hired by parents.

<u>Governing Body, led by Safeguarding Link Governor</u>

Key responsibilities (quotes are taken from Keeping Children Safe in Education)

- Approve this policy and strategy.
- Undergo (and signpost all other governors to attend) safeguarding and child protection training (including online safety) at induction to provide strategic challenge and into policy and practice, ensuring this is regularly updated.
- Ensure that all staff also receive appropriate safeguarding and child protection (including online) training at induction and that this is updated.
- Appoint a filtering and monitoring governor to work closely with the DSL on the new filtering and monitoring standards
- Support the school in encouraging parents and the wider community to become engaged in online safety activities.
- Have regular strategic reviews with the online safety coordinator / DSL and incorporate online safety into standing discussions of safeguarding at governor meetings.
- Work with the DPO, DSL and headteacher to ensure a compliant framework for storing data but helping to ensure that child protection is always put first, and data-protection processes support careful and legal sharing of information.
- Check all school staff have read Part 1 of KCSIE; SLT and all working directly with children have read **APPENDIX B**.
- Ensure that all staff undergo safeguarding and child protection training (including online safety and now also reminders about filtering and monitoring.
- "Ensure that children are taught about safeguarding, including online safety […] as part of providing a broad and balanced curriculum […] Consider a whole school or college

approach to online safety [with] a clear policy on the use of mobile technology.

REACH Lead

Key responsibilities:

- As listed in the 'all staff' section, plus:
- Embed consent, mental wellbeing, healthy relationships and staying safe online as well as raising awareness of the risks and challenges from latest trends in self-generative artificial intelligence, financial extortion and sharing intimate pictures online into the PSHE / Relationships education, relationships and sex education (RSE) and health education curriculum. "This will include being taught what positive, healthy and respectful online relationships look like, the effects of their online actions on others and knowing how to recognise and display respectful behaviour online. Throughout these subjects, teachers will address online safety and appropriate behaviour in an age-appropriate way that is relevant to their pupils' lives."
- Help pupils to navigate the online world safely and confidently regardless of their device, platform or app.
- Work closely with the DSL and all other staff to ensure an understanding of the issues, approaches and messaging within REACH.
- Work closely with the Computing subject leader to avoid overlap but ensure a complementary whole-school approach, and with all other lead staff to embed the same whole-school approach.

Computing Lead

Key responsibilities:

- As listed in the 'all staff' section, plus:
- Oversee the delivery of the online safety element of the Computing curriculum in accordance with the national curriculum.
- Work closely with the RSHE lead to avoid overlap but ensure a complementary whole-school approach.
- Work closely with the DSL/OSL and all other staff to ensure an understanding of the issues, approaches and messaging within Computing.
- Collaborate with technical staff and others responsible for ICT use in school to ensure a common and consistent approach, in line with acceptable-use agreements.

Subject/Faculty leaders

Key responsibilities:

- As listed in the 'all staff' section, plus:
- Look for opportunities to embed online safety in your subject or aspect, especially as part of the RSHE curriculum, and model positive attitudes and approaches to staff and pupils alike.
- Consider how the UKCIS framework Education for a Connected World and Teaching Online Safety in Schools can be applied in your context.

- Work closely with the DSL/OSL and all other staff to ensure an understanding of the issues, approaches and messaging within Computing.
- Ensure subject specific action plans also have an online safety element.

Network Manager/other technical support roles – BCTEC

Key responsibilities:

- As listed in the 'all staff' section, plus:
- Collaborate regularly with the DSL and leadership team to help them make key strategic decisions around the safeguarding elements of technology.
- Support safeguarding teams to understand and manage filtering and monitoring systems and carry out regular reviews and annual checks
- Support DSLs and SLT to carry out an annual online safety audit as recommended in KCSIE.
- This should also include a review of technology, including filtering and monitoring systems (what is allowed, blocked and why and how 'over blocking' is avoided as per KCSIE) to support their role as per the DfE standards, protections for pupils in the home and remote learning.
- Keep up to date with the school's online safety policy and technical information in order to effectively carry out their online safety role and to inform and update others as relevant.
- Work closely with the designated safeguarding lead / online safety lead / data protection officer / LGfL nominated contact / RSHE lead to ensure that school systems and networks reflect school policy and there are no conflicts between educational messages and practice.
- Ensure the above stakeholders understand the consequences of existing services and of any changes to these systems (especially in terms of access to personal and sensitive records / data and to systems such as YouTube mode, web filtering settings, sharing permissions for files on cloud platforms etc.
- Ensure filtering and monitoring systems work on new devices and services before releasing them to students and staff.
- Maintain up-to-date documentation of the school's online security and technical procedures.
- To report online safety related issues that come to their attention in line with school policy.
- Manage the school's systems, networks and devices, according to a strict password policy, with systems in place for detection of misuse and malicious attack, with adequate protection, encryption and backup for data, including disaster recovery plans, and auditable access controls.
- Ensure the data protection policy and cyber security policy are up to date, easy to follow and practicable
- Monitor the use of school technology, online platforms and social media presence and that any misuse/attempted misuse is identified and reported in line with school policy.
- Work with the Head of School to ensure the school website meets statutory DfE requirements.

Data Protection Officer (DPO) - Outsourced to Bulletproof

Key responsibilities:

- Alongside those of other staff, provide data protection expertise and training and support the DP and cyber security policy and compliance with those and legislation and ensure that the policies conform with each other and with this policy.
- Not prevent, or limit, the sharing of information for the purposes of keeping children safe. As outlined in *Data protection in schools*, 2023, "It's not usually necessary to ask for consent to share personal information for the purposes of safeguarding a child." And in KCSIE, "The Data Protection Act 2018 and UK GDPR do not prevent the sharing of information for the purposes of keeping children safe. Fears about sharing information must not be allowed to stand in the way of the need to safeguard and promote the welfare and protect the safety of children."
- Ensure that all access to safeguarding data is limited as appropriate and also monitored and audited.

Volunteers and contractors (including tutors)

Key responsibilities:

- Read, understand, sign and adhere to an Acceptable Use Policy (AUP)
- Report any concerns, no matter how small, to the designated safety lead.
- Maintain an awareness of current online safety issues and guidance.
- Model safe, responsible and professional behaviours in their own use of technology at school and as part of remote teaching or any online communications.
- Note that as per AUP agreement a contractor will never attempt to arrange any meeting, **including tutoring session,** without the full prior knowledge and approval of the school, and will never do so directly with a pupil. The same applies to any private/direct communication with a pupil.

Pupils

Key responsibilities:

Read, understand, sign and adhere to the student acceptable use policy.

Parents/carers

Key responsibilities:

- Read, sign and adhere to the school's parental acceptable use policy (AUP), read the pupil AUP and encourage their children to follow it.

External groups (e.g. those hiring the premises) including parent associations

Key responsibilities:

- Any external individual/organisation will sign an acceptable use policy prior to using technology or the internet within school.
- Support the school in promoting online safety and data protection.
- Model safe, responsible, respectful and positive behaviours in their own use of technology, including on social media: not sharing other's images or details without permission and refraining from posting negative, threatening or violent comments about others, including the school staff, volunteers, governors, contractors, pupils or other parents/carers.

Appendix B – Acceptable Use

User actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Users shall not access online content (including apps, games, sites) to make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	**Any illegal activity for example:** • Child sexual abuse imagery* • Child sexual abuse/exploitation/grooming • Terrorism • Encouraging or assisting suicide • Offences relating to sexual images i.e., revenge and extreme pornography • Incitement to and threats of violence • Hate crime • Public order offences - harassment and stalking • Drug-related offences • Weapons / firearms offences • Fraud and financial crime including money laundering					X
Users shall not undertake activities that might be classed as cyber-crime under the Computer Misuse Act (1990)	• Using another individual's username or ID and password to access data, a program, or parts of a system that the user is not authorised to access (even if the initial access is authorised) • Gaining unauthorised access to school networks, data and files, through the use of computers/devices • Creating or propagating computer viruses or other harmful files • Revealing or publicising confidential or proprietary information (e.g., financial / personal information, databases, computer / network access codes and passwords) • Disable/Impair/Disrupt network functionality through the use of computers/devices • Using penetration testing equipment (without relevant permission)					X
Users shall not undertake activities that are not illegal but are classed as unacceptable in school policies:	Accessing inappropriate material/activities online in a school setting including pornography, gambling, drugs. (Informed by the school's filtering practices and/or AUAs)				X	
	Promotion of any kind of discrimination				X	
	Using school systems to run a private business				X	

	Using systems, applications, websites or other mechanisms that bypass the filtering/monitoring or other safeguards employed by the school				X	
	Infringing copyright and intellectual property (including through the use of AI services)				X	
	Unfair usage (downloading/uploading large files that hinders others in their use of the internet)				X	
	Any other information which may be offensive to others or breaches the integrity of the ethos of the school or brings the school into disrepute				X	

Consideration should be given for the following activities when undertaken for non-educational purposes: Schools may wish to add further activities to this list.	**Staff and other adults**				**Learners**			
	Not allowed	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission/awareness
Online gaming	X				X			
Online shopping/commerce			X		X			
File sharing				X			X	
Social media				X	X			
Messaging/chat		X					X	
Entertainment streaming e.g. Netflix, Disney+			X		X			
Use of video broadcasting, e.g. YouTube, Twitch, TikTok				X			X	

Mobile phones may be brought to school		X					X	
Use of mobile phones for learning at school	X				X			
Use of mobile phones in social time at school			X		X			
Taking photos on mobile phones/cameras	X				X			
Use of other personal devices, e.g. tablets, gaming devices	X				X			
Use of personal e-mail in school, or on school network/wi-fi	X				X			
Use of school e-mail for personal e-mails	X				X			
Use of AI services that have not been approved by the school	X				X			

Acronyms

LGFL	London Grid for Learning
WSGFL	West Sussex Grid for Learning
JAMF	Apple Device Management & Security
AUP	Acceptable Usage Policy
UKCIS	UK Council for Internet Security
DSL	Designated Safeguarding Lead
DPO	Data Protection Officer
DFE	Department for Education
AI	Artificial Intelligence
OSL	Online Safety Lead