CHARTERHOUSE

ONLINE SAFETY POLICY

Author: DH Safeguarding | **Reviewer**: DSL| **Last reviewed**: Sept 2026 | **Next Review**: Sept 2027

NUMEROUS UPDATES – INCLUDING ADDITION OF NEW APPENDIX GUIDE TO USE OF SOCIAL MEDIA FOR STAFF, PUPILS AND PARENTS

CHARTERHOUSE

ONLINE SAFETY POLICY

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

SCOPE OF THE ONLINE SAFETY POLICY

This Online Safety Policy outlines the commitment of Charterhouse to safeguard members of our School community online in accordance with statutory guidance and best practice. The School are aware of the legislative framework under which this Online Safety Policy template and guidance has been produced as outlined in the attached 'Legislation' Appendix. The School also recognise digital technology and the internet are amazing resources which bring exciting new experience, learning opportunities and methods of communication.

This Online Safety Policy applies to all members of the School community (including staff, pupils, governors, volunteers, parents and guardians, visitors, community users) who have access to and are users of School digital systems, both in and out of the School. It also applies to the use of personal digital technology on the School site (where permitted).

Charterhouse will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents/guardians of incidents of inappropriate online safety behaviour that take place out of School.

POLICY DEVELOPMENT, MONITORING, AND REVIEW

This Online Safety Policy has been developed with input from the Online Safety Group, and nominated governors.

Consultation with the whole School community has taken place through a range of formal and informal meetings and the annual safeguarding audit.

SCHEDULE FOR DEVELOPMENT, MONITORING, AND REVIEW

This Online Safety Policy was first approved by the *School governing body on:*	*October 10, 2023*
The implementation of this Online Safety Policy will be monitored by:	*Designated Safeguarding Lead*
Monitoring will take place at regular intervals:	*Annually or earlier if needed*
The G*overning Body* will receive a report on the implementation of the Online Safety Policy generated by the monitoring group (which will include anonymous details of online safety incidents) at regular intervals:	*Annually or earlier in the event of a significant issue*
The Online Safety Policy will be reviewed annually, or more regularly in the light of any significant new technological developments, new threats to online safety or incidents that have taken place. The next anticipated review date will be:	*September 2027 or earlier*
Should serious online safety incidents take place, the following external persons/agencies should be informed:	*LA, LADO, Police, Internet Watch Foundation*

PROCESS FOR MONITORING THE IMPACT OF THE ONLINE SAFETY POLICY

The School will monitor the impact of the policy using:

- *logs of reported incidents*
- *Filtering and monitoring logs*
- *internal monitoring data for network activity*
- *surveys/questionnaires of:*
    - *pupils*
    - *parents and guardians*
    - *staff.*

POLICY AND LEADERSHIP

Responsibilities

To ensure the online safeguarding of members of our School community it is important that all members of that community work together to develop safe and responsible online behaviours, learning from each other and from good practice elsewhere, reporting inappropriate online behaviours, concerns, and misuse as soon as these become apparent. While this will be a team effort, the following sections outline the online safety roles and responsibilities of individuals and groups within the School.

The Head and senior leaders

- The Head and CEO has a duty of care for ensuring the safety (including online safety) of members of the School community and fostering a culture of safeguarding, though the day-to-day responsibility

for online safety is held by the Designated Safeguarding Lead, as defined in Keeping Children Safe in Education.

- The Head and CEO should be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff.
- The Head and CEO/senior leaders are responsible for ensuring that the Designated Safeguarding Lead / Online Safety Lead, Director of IT, and other relevant staff carry out their responsibilities effectively and receive suitable training to enable them to carry out their roles and train other colleagues, as relevant.
- The Head and CEO/senior leaders will ensure that there is a system in place to allow for monitoring and support of those in School who carry out the internal online safety monitoring role.
- The Head and CEO/senior leaders will receive regular monitoring reports from the Designated Safeguarding Lead / Online Safety Lead.
- The Head and CEO/senior leaders will work with the responsible Governor, the Designated Safeguarding Lead (DSL) and Director of IT in all aspects of filtering and monitoring.

Governors

The DfE guidance "Keeping Children Safe in Education" states:
"Governing bodies and proprietors should ensure there are appropriate policies and procedures in place in order for appropriate action to be taken in a timely manner to safeguard and promote children's welfare …. this includes … online safety"

"Governing bodies and proprietors should ensure an appropriate senior member of staff, from the School or college leadership team, is appointed to the role of designated safeguarding lead. The designated safeguarding lead should take lead responsibility for safeguarding and child protection (including online safety and understanding the filtering and monitoring systems and processes in place)"

Governors are responsible for the approval of the Online Safety Policy and for reviewing the effectiveness of the policy e.g. by asking the questions posed in the UKCIS document "Online Safety in Schools and Colleges – questions from the Governing Body".

This review will be carried out by the Safeguarding Governor and Online Safety Governor who will receive regular information about online safety incidents and monitoring reports.

A member of the governing body will take on the role of Online Safety Governor to include:

- Regular meetings with the Designated Safeguarding Lead / Online Safety Lead
- Regularly receiving (collated and anonymised) reports of online safety incidents
- Checking that provision outlined in the Online Safety Policy (e.g., online safety education provision and staff training is taking place as intended)
- Ensuring that the filtering and monitoring provision is reviewed and recorded, at least annually. (The review will be conducted by members of the SLT, the DSL, and the Director of IT and involve the responsible governor) in-line with the DfE Filtering and Monitoring Standards
- Reporting to Safeguarding Committee
- Receiving (at least) basic cyber-security training to enable the governors to check that the School meets the DfE Cyber-Security Standards
- Membership of the School Online Safety Group

The governing body will also support the School in encouraging parents/guardians and the wider community to become engaged in online safety activities.

Designated Safety Lead (DSL)

Keeping Children Safe in Education states that:

> *"The designated safeguarding lead should take lead responsibility for safeguarding and child protection (including online safety and understanding the filtering and monitoring systems and processes in place). This should be explicit in the role holder's job description."*

They (the DSL) "are able to understand the unique risks associated with online safety and be confident that they have the relevant knowledge and up to date capability required to keep children safe whilst they are online at School or college"

They (the DSL) *"*can recognise the additional risks that children with special educational needs and disabilities (SEND) face online, for example, from bullying, grooming and radicalisation and are confident they have the capability to support children with SEND to stay safe online"

While the responsibility for online safety is held by the DSL and cannot be delegated, the School may choose to appoint an Online Safety Lead or other relevant persons to work in support of the DSL in carrying out these responsibilities. It is recommended that the School reviews the sections below for the DSL and OSL and allocate roles depending on the structure it has chosen

The DSL will:

- Hold the lead responsibility for online safety, within their safeguarding role and have responsibility for the strategic leadership the Online Safety Group
- Receive relevant and regularly updated training in online safety to enable them to understand the risks associated with online safety and be confident that they have the relevant knowledge and up to date capability required to keep children safe whilst they are online
- Meet regularly with the online safety governor to discuss current issues, review (anonymised) incidents and filtering and monitoring logs and ensuring that annual (at least) filtering and monitoring checks are carried out
- Attend relevant governing body meetings/groups
- Report regularly to Head/Senior Leadership Team
- Be responsible for receiving reports of online safety incidents and handling them and deciding whether to make a referral by liaising with relevant agencies, ensuring that all incidents are recorded.
- Liaise with staff and Director of IT on matters of safety and safeguarding and welfare (including online and digital safety)
- Have a leading role in establishing and reviewing the School online safety policies/documents
- Provide (or identify sources of) training and advice for staff/governors/parents/guardians/pupils

Online Safety DDSL

The Online Safety Lead will:

- Work closely on a day-to-day basis with the Designated Safeguarding Lead (DSL)
- Receive reports of online safety issues, being aware of the potential for serious child protection concerns and ensure that these are logged to inform future online safety developments
- Promote an awareness of and commitment to online safety education / awareness raising across the School and beyond
- Liaise with curriculum leaders to ensure that the online safety curriculum is planned, mapped, embedded and evaluated

- Ensure that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place and the need to immediately report those incidents
- Liaise with technical staff, pastoral staff and support staff (as relevant)
- Receive regularly updated training to allow them to understand how digital technologies are used and are developing (particularly by pupils) about the areas defined in Keeping Children Safe in Education:
    - content
    - contact
    - conduct
    - commerce

Heads of Department and Heads of House?

Heads of Department will work with the DSL/OSL to develop a planned and coordinated online safety education programme.

This will be provided through:

- PSHE, Computing and SRE programmes
- A mapped cross-curricular programme
- Assemblies and pastoral programmes
- Through relevant national initiatives and opportunities e.g. Safer Internet Day and Anti-bullying week.

Teaching and support staff

School staff are responsible for ensuring that:

- They have an awareness of current online safety matters/trends and of the current School Online Safety Policy and practices
- They understand that online safety is a core part of safeguarding
- They have read, understood, and signed the Staff Acceptable Use Agreement
- They immediately report any suspected misuse or problem to the DSL for investigation/action, in line with the School safeguarding procedures
- All digital communications with pupils and parents/guardians are on a professional level and only carried out using appropriate and official School systems
- Online safety issues are embedded in all aspects of the curriculum and other activities
- Ensure pupils understand and follow the Online Safety Policy and acceptable use agreements, have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- They supervise and monitor the use of digital technologies, mobile devices, cameras, etc., in lessons and other School activities (where allowed) and implement current policies regarding these devices
- In lessons where internet use is pre-planned pupils are guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches
- Where lessons take place using live-streaming or videoconferencing, there is regard to national safeguarding guidance and local safeguarding policies
- There is a zero-tolerance approach to incidents of online-bullying, sexual harassment, discrimination, hatred etc

- They model safe, responsible, and professional online behaviours in their own use of technology, including out of School and in their use of social media.

IT Department
The DfE Filtering and Monitoring Standards says:

"Senior leaders should work closely with governors or proprietors, the designated safeguarding lead (DSL) and IT service providers in all aspects of filtering and monitoring. Your IT service provider may be a staff technician or an external service provider."

"Day to day management of filtering and monitoring systems requires the specialist knowledge of both safeguarding and IT staff to be effective. The DSL should work closely together with IT to meet the needs of your setting. You may need to ask filtering or monitoring providers for system specific training and support."

"The IT Department should have technical responsibility for:

- maintaining filtering and monitoring systems
- providing filtering and monitoring reports
- completing actions following concerns or checks to systems"

"The IT Department should work with the senior leadership team and DSL to:

- procure systems
- identify risk
- carry out reviews
- carry out checks"

The IT Department is responsible for ensuring that:

- They are aware of and follow the School Online Safety Policy and IT Online Safety and Technical Security Policy to carry out their work effectively in line with School policy
- The School technical infrastructure is secure and is not open to misuse or malicious attack
- The School meets (as a minimum) the required online safety technical requirements as identified by the DfE Meeting Digital and Technology Standards in Schools & Colleges and guidance from local authority.
- There is clear, safe, and managed control of user access to networks and devices
- They keep up to date with online safety technical information to effectively carry out their online safety role and to inform and update others as relevant
- The use of technology is regularly and effectively monitored in order that any misuse/attempted misuse can be reported to the DSL or OSL for investigation and action
- The filtering policy is applied and updated on a regular basis and its implementation is not the sole responsibility of any single person (see appendix 'Technical Security Policy template' for good practice).
- Monitoring systems are implemented and regularly updated as agreed in School policies

Pupils

- Are responsible for using the School digital technology systems in accordance with the learner acceptable use agreement and Online Safety Policy (this should include personal devices – where allowed)

- Should understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- Should know what to do if they or someone they know feels vulnerable when using online technology.
- Should understand the importance of adopting good online safety practice when using digital technologies out of School and realise that the School's Online Safety Policy covers their actions out of School, if related to their membership of the School.

Parents and guardians

Parents and guardians play a crucial role in ensuring that their children understand the need to use the online services and devices in an appropriate way.

The School will take every opportunity to help parents and guardians understand these issues through:

- Publishing the School Online Safety Policy on the School website
- Providing them with a copy of the pupils' acceptable use agreement
- Publish information about appropriate use of social media relating to posts concerning the School.
- Seeking their permissions concerning digital images, cloud services etc
- Parents'/guardians' meetings, newsletters, website, social media and information about national/local online safety campaigns and literature

Parents and guardians will be encouraged to support the School in:

- Reinforcing the online safety messages provided to pupils in School.
- The safe and responsible use of their children's personal devices in the School (where this is allowed)

Visitors should refer to the Visitor and Contractor policy.

Online Safety Group

The Online Safety Group provides a consultative group that has wide representation from the School community, with responsibility for issues regarding online safety and monitoring the Online Safety Policy including the impact of initiatives. The group will also be responsible for regular reporting to senior leaders and the governing body.

The Online Safety Group has the following members:

- Designated Safeguarding Lead
- DDSL
- Director of IT
- Assistant Head (Under School)
- Head of Informatics and Computer Science
- Online Safety Governor

Members of the Online Safety Group will assist the DSL with:

- the production/review/monitoring of the School Online Safety Policy/documents
- the production/review/monitoring of the School filtering policy and requests for filtering changes
- mapping and reviewing the online safety education provision – ensuring relevance, breadth and progression and coverage
- reviewing network/filtering/monitoring/incident logs, where possible
- encouraging the contribution of pupils to staff awareness, emerging trends and the School online safety provision
- consulting stakeholders – including staff/parents/guardians about the online safety provision
- monitoring improvement actions identified through use of the 360-degree safe self-review tool.

Professional Standards

There is an expectation that required professional standards will be applied to online safety as in other aspects of School life i.e., policies and protocols are in place for the use of online communication technology between the staff and other members of the School and wider community, using officially sanctioned School mechanisms.

Online Safety Policy

The DfE guidance "Keeping Children Safe in Education" states:
"Online safety and the School or college's approach to it should be reflected in the child protection policy"

The School Online Safety Policy:

- sets expectations for the safe and responsible use of digital technologies for learning, administration, and communication
- allocates responsibilities for the delivery of the policy
- is regularly reviewed in a collaborative manner, taking account of online safety incidents and changes/trends in technology and related behaviours
- establishes guidance for staff in how they should use digital technologies responsibly, protecting themselves and the School and how they should use this understanding to help safeguard pupils in the digital world
- describes how the School will help prepare pupils to be safe and responsible users of online technologies

- establishes clear procedures to identify, report, respond to and record the misuse of digital technologies and online safety incidents, including external support mechanisms
- is supplemented by a series of related acceptable use agreements
- is made available to staff at induction and through normal communication channels
- is published on the School website.

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. They are acknowledged by all staff as part of their conditions of employment. Pupils and parents/guardians also acknowledge them, and these are regularly promoted, understood and followed rather than just signed. The acceptable use agreements are in the appendices.

The Online Safety Policy and acceptable use agreements define acceptable use at the School. The acceptable use agreements will be communicated/re-enforced through:

- pupil induction booklet
- staff induction and handbook
- posters/notices around where technology is used
- communication with parents/guardians
- built into education sessions
- School website
- School intranet

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 N.B. Schools should refer to guidance about dealing with self-generated images/sexting – UKSIC Responding to and managing sexting incidents and UKCIS – Sexting in Schools and colleges					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,					X

User actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
	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) N.B. Schools will need to decide whether these should be dealt with internally or by the police. Serious or repeat offences should be reported to the police. The National Crime Agency has a remit to prevent pupils becoming involved in cyber-crime and harness their activity in positive ways– further information here					
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	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				X	
	Unfair usage (downloading/uploading large files that hinders others in their use of the internet)			X	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				Pupils			
	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								
Online shopping/commerce								
File sharing								
Social media								
Messaging/chat								
Entertainment streaming e.g. Netflix, Disney+								
Use of video broadcasting, e.g. YouTube, Twitch, TikTok								
Mobile phones may be brought to School								
Use of mobile phones for learning at School								
Use of mobile phones in social time at School								
Taking photos on mobile phones/cameras								
Use of other personal devices, e.g. tablets, gaming devices								

Use of personal e-mail in School, or on School network/wi-fi								
Use of School e-mail for personal e-mails								

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 pupils or parents/guardians (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 pupils.

Reporting and responding

The 2021 Ofsted "Review of Sexual Abuse in Schools and Colleges" highlighted the need for Schools to understand that reporting systems do not always respond to the needs of pupils. While the report looks specifically at harmful sexual behaviours, Schools may wish to address these issues more generally in reviewing their reporting systems. The Ofsted review suggested:

"School and college leaders should create a culture where sexual harassment and online sexual abuse are not tolerated, and where they identify issues and intervene early to better protect children and young people. In order to do this, they should assume that sexual harassment and online sexual abuse are happening in their setting, even when there are no specific reports, and put in place a whole-School approach to address them. This should include:

  - routine record-keeping and analysis of sexual harassment and sexual violence, including online, to identify patterns and intervene early to prevent abuse"

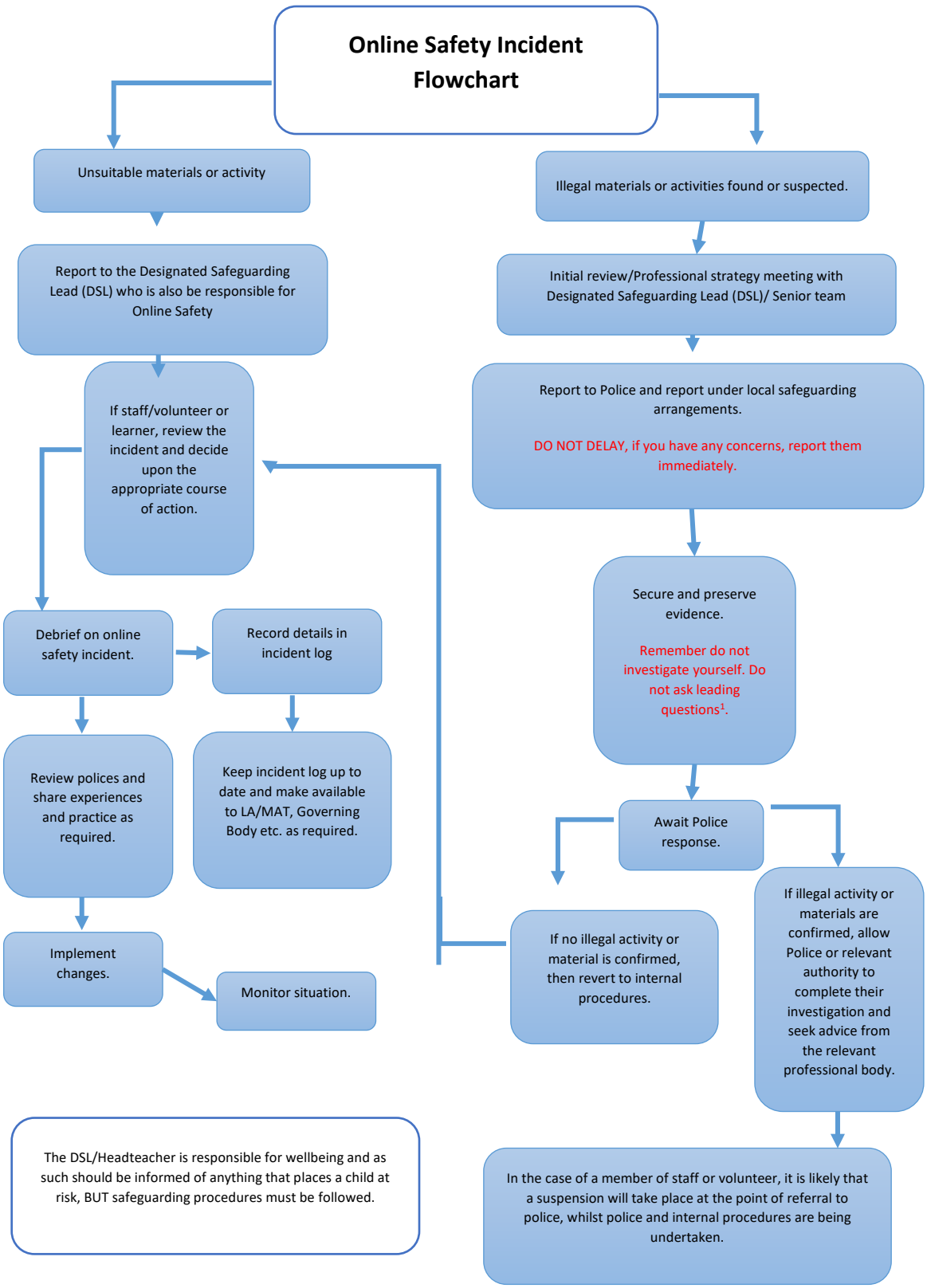
The School will take all reasonable precautions to ensure online safety for all School users but recognises that incidents may occur inside and outside of the School (with impact on the School) which will need intervention. The School will ensure:

- there are clear reporting routes which are understood and followed by all members of the School community which are consistent with the School safeguarding procedures, and with the whistleblowing, complaints and managing allegations policies. At Charterhouse, we use online/anonymous reporting systems SWGfL Whisper

- all members of the School community will be made aware of the need to report online safety issues/incidents
- reports will be dealt with as soon as is practically possible once they are received
- the Designated Safeguarding Lead and other responsible staff have appropriate skills and training to deal with online safety risks.
- if there is any suspicion that the incident involves any illegal activity or the potential for serious harm (see flowchart and user actions chart in the appendix), the incident must be escalated through the agreed School safeguarding procedures, this may include:
    - Non-consensual images
    - Self-generated images
    - Terrorism/extremism
    - Hate crime/ Abuse
    - Fraud and extortion
    - Harassment/stalking
    - Child Sexual Abuse Material (CSAM)
    - Child Sexual Exploitation Grooming
    - Extreme Pornography
    - Sale of illegal materials/substances
    - Cyber or hacking offences under the Computer Misuse Act
    - Copyright theft or piracy
- any concern about staff misuse will be reported to the DSL, unless the concern involves the DSL, in which case the complaint is referred to the Principal Deputy Head and the local authority.
- where there is no suspected illegal activity, devices may be checked using the following procedures:
    - one or more senior members of staff should be involved in this process. This is vital to protect individuals if accusations are subsequently reported.
    - conduct the procedure using a designated device that will not be used by pupils and, if necessary, can be taken off site by the police should the need arise (should illegal activity be subsequently suspected). Use the same device for the duration of the procedure.
    - ensure that the relevant staff have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
    - record the URL of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed, and attached to the form. Once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does, then appropriate action will be required and could include the following:
        - internal response or discipline procedures
        - police involvement and/or action
- it is important that those reporting an online safety incident have confidence that the report will be treated seriously and dealt with effectively
- there are support strategies in place e.g., peer support for those reporting or affected by an online safety incident
- incidents should be logged in the reporting log see appendix

- relevant staff are aware of external sources of support and guidance in dealing with online safety issues, e.g., local authority; police; Professionals Online Safety Helpline; Reporting Harmful Content; CEOP.
- those involved in the incident will be provided with feedback about the outcome of the investigation and follow up actions (as relevant)
- learning from the incident (or pattern of incidents) will be provided (as relevant and anonymously) to:
    - the Online Safety Group for consideration of updates to policies or education programmes and to review how effectively the report was dealt with
    - staff, through regular briefings
    - pupils, through assemblies/lessons
    - parents/guardians, through newsletters, School social media, website
    - governors, through regular safeguarding updates
    - local authority/external agencies, as relevant (The Ofsted Review into Sexual Abuse in Schools and Colleges suggested "working closely with Local Safeguarding Partnerships in the area where the School or college is located so they are aware of the range of support available to children and young people who are victims or who perpetrate harmful sexual behaviour"

The School will make the flowchart below available to staff to support the decision-making process for dealing with online safety incidents.


Online Safety Incident Flowchart
Unsuitable materials or activity
Illegal materials or activities found or suspected.
Report to the Designated Safeguarding Lead (DSL) who is also be responsible for Online Safety
Initial review/Professional strategy meeting with Designated Safeguarding Lead (DSL)/ Senior team
If staff/volunteer or learner, review the incident and decide upon the appropriate course of action.
Report to Police and report under local safeguarding arrangements.
DO NOT DELAY, if you have any concerns, report them immediately.
Debrief on online safety incident.
Record details in incident log
Secure and preserve evidence.
Remember do not investigate yourself. Do not ask leading questions[1].
Review polices and share experiences and practice as required.
Keep incident log up to date and make available to LA/MAT, Governing Body etc. as required.
Await Police response.
Implement changes.
Monitor situation.
If no illegal activity or material is confirmed, then revert to internal procedures.
If illegal activity or materials are confirmed, allow Police or relevant authority to complete their investigation and seek advice from the relevant professional body.
The DSL/Headteacher is responsible for wellbeing and as such should be informed of anything that places a child at risk, BUT safeguarding procedures must be followed.
In the case of a member of staff or volunteer, it is likely that a suspension will take place at the point of referral to police, whilst police and internal procedures are being undertaken.

School actions

It is more likely that the School will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the School community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal behaviour/disciplinary procedures as follows: (the School will need to agree upon its own responses and place the ticks in the relevant columns. They may also wish to add additional text to the column(s) on the left to clarify issues. Schools have found it useful to use the charts below at staff meetings/training sessions)

Responding to Learner Actions

Incidents	Refer to class teacher/tutor	Refer to Head of House / Deputy Head	Refer to Head	Refer to Police/Social Work	Refer to local authority technical support for advice/action	Inform parents/guardians	Remove device/ network/internet access	Issue a warning	Further sanction, in line with behaviour policy
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on User Actions on unsuitable/inappropriate activities).		X		X		X	X		X
Attempting to access or accessing the School network, using another user's account (staff or learner) or allowing others to access School network by sharing username and passwords		X				X	X		X
Corrupting or destroying the data of other users.		X				X	X		X
Sending an e-mail, text or message that is regarded as offensive, harassment or of a bullying nature		X				X			X
Unauthorised downloading or uploading of files or use of file sharing.		X				X			X

Using proxy sites or other means to subvert the School's filtering system.		X						X	
Accidentally accessing offensive or pornographic material and failing to report the incident.		X						X	X
Deliberately accessing or trying to access offensive or pornographic material.		X				X		X	X
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act.		X				X		X	X
Unauthorised use of digital devices (including taking images)		X				X		X	X
Unauthorised use of online services		X						X	
Actions which could bring the School into disrepute or breach the integrity or the ethos of the School.		X				X		X	X
Continued infringements of the above, following previous warnings or sanctions.		X	X	X	X	X	X	X	X

Responding to Staff Actions

Incidents	Refer to line manager	Refer to Head/ DSL	Refer to local authority/MAT/HR	Refer to Police	Refer to LA / Technical Support Staff for action re filtering, etc.	Issue a warning	Suspension	Disciplinary action
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities)		X		X			X	X
Deliberate actions to breach data protection or network security rules.		X			X	X		X
Deliberately accessing or trying to access offensive or pornographic material		X		X	X			X
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software		X		X				X
Using proxy sites or other means to subvert the School's filtering system.		X			X			X
Unauthorised downloading or uploading of files or file sharing		X				X		
Breaching copyright or licensing regulations.		X				X		
Allowing others to access School network by sharing username and passwords or attempting to access or accessing the School network, using another person's account.	X				X	X		
Sending an e-mail, text or message that is regarded as offensive, harassment or of a bullying nature		X						
Using personal e-mail/social networking/messaging to carry out digital communications with pupils and parents/guardians	X					X		

Inappropriate personal use of the digital technologies e.g., social media / personal e-mail	X					X		
Careless use of personal data, e.g., displaying, holding or transferring data in an insecure manner	X					X		
Actions which could compromise the staff member's professional standing	X	X				X		X
Actions which could bring the School into disrepute or breach the integrity or the ethos of the School.	X	X						X
Failing to report incidents whether caused by deliberate or accidental actions	X					X		
Continued infringements of the above, following previous warnings or sanctions.		X					X	X

Online Safety Education Programme

While regulation and technical solutions are particularly important, their use must be balanced by educating pupils to take a responsible approach. The education of pupils in online safety is therefore an essential part of the School's online safety provision. Pupils need the help and support of the School to recognise and avoid online safety risks and develop their resilience.

The 2021 Ofsted "Review of Sexual Abuse in Schools and Colleges" highlighted the need for:
"a carefully sequenced RSHE curriculum, based on the Department for Education's (DfE's) statutory guidance, that specifically includes sexual harassment and sexual violence, including online. This should include time for open discussion of topics that children and young people tell us they find particularly difficult, such as consent and the sending of 'nudes'."

Keeping Children Safe in Education states:
"Governing bodies and proprietors should ensure online safety is a running and interrelated theme whilst devising and implementing their whole School or college approach to safeguarding and related policies and procedures. This will include considering how online safety is reflected as required in all relevant policies and considering online safety whilst planning the curriculum …"

Online safety should be a focus in all areas of the curriculum and staff should reinforce online safety messages across the curriculum. The online safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways:

- A planned online safety curriculum for all year groups matched against a nationally agreed framework e.g. Education for a Connected Work Framework by UKCIS/DCMS and the SWGfL Project Evolve and regularly taught in a variety of contexts.
- Lessons are matched to need; are age-related and build on prior learning
- Lessons are context-relevant with agreed objectives leading to clear and evidenced outcomes
- Learner need and progress are addressed through effective planning and assessment

- Digital competency is planned and effectively threaded through the appropriate digital pillars in other curriculum areas e.g., PHSE; SRE; Literacy etc
- it incorporates/makes use of relevant national initiatives and opportunities e.g. Safer Internet Day and Anti-bullying week
- the programme will be accessible to pupils at different ages and abilities such as those with additional learning needs or those with English as an additional language.
- vulnerability is actively addressed as part of a personalised online safety curriculum e.g., for victims of abuse and SEND.
- pupils should be helped to understand the need for the learner acceptable use agreement and encouraged to adopt safe and responsible use both within and outside School. Acceptable use is reinforced across the curriculum, with opportunities to discuss how to act within moral and legal boundaries online, with reference to the Computer Misuse Act 1990. Lessons and further resources are available on the CyberChoices site.
- staff should act as good role models in their use of digital technologies the internet and mobile devices
- in lessons where internet use is pre-planned, it is best practice that pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches
- where pupils are allowed to freely search the internet, staff should be vigilant in supervising the pupils and monitoring the content of the websites the young people visit
- it is accepted that from time to time, for good educational reasons, students may need to research topics, (e.g., racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff should be able to request the temporary removal of those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need
- the online safety education programme should be relevant and up to date to ensure the quality of learning and outcomes.

Contribution of Pupils

The School acknowledges, learns from, and uses the skills and knowledge of pupils in the use of digital technologies. We recognise the potential for this to shape the online safety strategy for the School community and how this contributes positively to the personal development of young people. Their contribution is recognised through our Safeguarding Pupil Action Committee.

And we are working towards:

- appointment of digital leaders/anti-bullying ambassadors/peer mentors
- the Online Safety Group has learner representation
- pupils contribute to the online safety education programme e.g., peer education, digital leaders leading lessons for younger pupils, online safety campaigns
- pupils designing/updating acceptable use agreements
- contributing to online safety events with the wider School community e.g., parents' meetings, family learning programmes etc.

Staff/volunteers

The DfE guidance "Keeping Children Safe in Education" states:

"All staff should receive appropriate safeguarding and child protection training (**including online safety**) at induction. The training should be **regularly updated**. In addition, all staff should receive safeguarding and child protection (**including online safety**) updates (for example, via email, e-bulletins, and staff meetings), as required, and at least annually, to continue to provide them with relevant skills and knowledge to safeguard children effectively."

"Governing bodies and proprietors should ensure... that safeguarding training for staff, **including online safety** training, is integrated, aligned and considered as part of the whole School or college safeguarding approach and wider staff training and curriculum planning.**"**

All staff will receive online safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- a planned programme of formal online safety and data protection training will be made available to all staff. This will be regularly updated and reinforced. An audit of the online safety training needs of all staff will be carried out regularly.
- the training will be an integral part of the School's annual safeguarding and data protection training for all staff
- all new staff will receive online safety training as part of their induction programme, ensuring that they fully understand the School online safety policy and acceptable use agreements. It includes explicit reference to classroom management, staff code of conduct, online reputation and the need to model positive online behaviours.
- the Designated Safeguarding Lead will receive regular updates through attendance at external training events, (e.g., UKSIC / SWGfL other relevant organisations) and by reviewing guidance documents released by relevant organisations
- this Online Safety Policy and its updates will be presented to and discussed by staff in staff/team meetings/INSET days
- the Designated Safeguarding Lead~~/Online Safety Lead~~ (or other nominated person) will provide advice/guidance/training to individuals as required.

Governors

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

- attendance at training provided by the local authority or other relevant organisation
- participation in School training / information sessions for staff or parents; this may include attendance at assemblies/lessons.

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

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

Families

Parents have varying degrees of understanding and engagement with online safety risks and issues, yet they play an essential role in the education of their children and in the monitoring/regulation of the children's online behaviours. Parents may underestimate how often children and young people come

across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.

The School will seek to provide information and awareness to parents and guardians through:

- regular communication, awareness-raising and engagement on online safety issues, curriculum activities and reporting routes
- regular opportunities for engagement with parents/guardians on online safety issues through awareness workshops / parent/guardian meetings etc
- the pupils – who are encouraged to pass on to parents the online safety messages they have learned in lessons and by pupils leading sessions at parent/guardian meetings.
- letters, newsletters, website, learning platform,
- high profile events / campaigns e.g., Safer Internet Day
- reference to the relevant web sites/publications, e.g. SWGfL; www.saferinternet.org.uk/; www.childnet.com/parents-and-guardians (see Appendix for further links/resources).
- Sharing good practice with other Schools in clusters and or the local authority

Adults and Agencies

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

- online safety messages targeted towards families and relatives.

Technology

The DfE Filtering and Monitoring Standards states that "Your IT service provider may be a staff technician or an external service provider"

The School is responsible for ensuring that the School infrastructure/network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. The School should ensure that all staff are made aware of policies and procedures in place on a regular basis and explain that everyone is responsible for online safety and data protection.

Filtering & Monitoring

The DfE guidance (for England) on filtering and monitoring in "Keeping Children Safe in Education" states:

"It is essential that governing bodies and proprietors ensure that appropriate filtering and monitoring systems are in place governing bodies and proprietors should be doing all that they reasonably can to limit children's exposure to the risks from the School's IT system. As part of this process, governing bodies and proprietors should ensure their School has appropriate filtering and monitoring systems in place and regularly review their effectiveness. They should ensure that the leadership team and relevant staff have an awareness and understanding of the provisions in place and manage them effectively and know how to escalate concerns when identified.

The appropriateness of any filtering and monitoring systems are a matter for individual Schools and colleges and will be informed in part, by the risk assessment required by the Prevent Duty. To support Schools and colleges to meet this duty, the Department for Education has published filtering and monitoring standards.

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

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

The filtering and monitoring provision is reviewed at least annually by senior leaders, the Designated Safeguarding Lead and a governor with the involvement of the IT Service Provider.

- checks on the filtering and monitoring system are carried out by the IT Department with the involvement of a senior leader, the Designated Safeguarding Lead and a governor, when a safeguarding risk is identified, there is a change in working practice, e.g., remote access or BYOD or new technology is introduced e.g., using SWGfL Test Filtering

Filtering

- the School manages access to content across its systems for all users and on all devices using the School's internet provision. The filtering provided meets the standards defined in the DfE Filtering standards for Schools and colleges and the guidance provided in the UK Safer Internet Centre Appropriate filtering.
- illegal content (e.g., child sexual abuse images) is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation URL list and the police assessed list of unlawful terrorist content, produced on behalf of the Home Office. Content lists are regularly updated
- there are established and effective routes for users to report inappropriate content, recognising that no system can be 100% effective
- there is a clear process in place to deal with, and log, requests/approvals for filtering changes (see Appendix for more details).
- filtering logs are regularly reviewed and alert the Designated Safeguarding Lead to breaches of the filtering policy, which are then acted upon.
- the School has (if possible) provided enhanced/differentiated user-level filtering (allowing different filtering levels for different abilities/ages/stages and different groups of users: staff/pupils, etc.). Currently, only for staff and pupils.
- the School has a mobile phone policy and where personal mobile devices have internet access through the School network, content is managed in ways that are consistent with School policy and practice.
- access to content through non-browser services (e.g., apps and other mobile technologies) is managed in ways that are consistent with School policy and practice.

If necessary, the School will seek advice from, and report issues to, the SWGfL Report Harmful Content site.

Monitoring

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

- The School monitors all network use across all its devices and services.
- monitoring reports are urgently picked up, acted on and outcomes are recorded by the Designated Safeguarding Lead, all users are aware that the network (and devices) are monitored.
- There are effective protocols in place to report abuse/misuse. There is a clear process for prioritising response to alerts that require rapid safeguarding intervention.

- Management of serious safeguarding alerts is consistent with safeguarding policy and practice.

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

- physical monitoring (adult supervision in the classroom)
- internet use is logged, regularly monitored and reviewed
- filtering logs are regularly analysed, and breaches are reported to senior leaders
- pro-active alerts inform the School of breaches to the filtering policy, allowing effective intervention.
- School technical staff regularly monitor and record the activity of users on the School technical systems
- use of a third-party assisted monitoring service to review monitoring logs and report issues to School monitoring lead(s)

Technical Security

Charterhouse have adopted a more detailed technical security policy which can be found at appendix C1.

The School technical systems are managed in ways that ensure that the School meets recommended technical requirements:

- responsibility for technical security resides with SLT who may delegate activities to identified roles.
- all users have clearly defined access rights to School technical systems and devices. Details of the access rights available to groups of users will be recorded by the IT service provider and will be reviewed, at least annually, by the SLT/Online Safety Group
- password policy and procedures are implemented which are consistent with guidance from the National Cyber Security Centre
- all users have responsibility for the security of their username and password and must not allow other users to access the systems using their log on details.
- all School networks and system are protected by secure passwords. Passwords must not be shared with anyone. (see section on passwords in 'Technical security policy'.
- the administrator passwords for School systems are kept in a secure place, e.g., School safe.
- there is a risk-based approach to the allocation of learner usernames and passwords.
- there will be regular reviews and audits of the safety and security of School technical systems
- servers, wireless systems and cabling are securely located and physical access restricted
- appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems and devices from accidental or malicious attempts which might threaten the security of the School systems and data. These are tested regularly. The School infrastructure and individual workstations are protected by up-to-date endpoint software.
- there are rigorous and verified back-up routines, including the keeping of network-separated (air-gapped) copies off-site or in the cloud,
- Head of I.T. is responsible for ensuring that all software purchased by and used by the School is adequately licenced and that the latest software updates (patches) are applied.
- an appropriate system is in place for users to report any actual/potential technical incident/security breach to the relevant person, as agreed)
- use of School devices out of School and by family members is regulated by an acceptable use statement that a user consents to when the device is allocated to them

- personal use of any device on the School network is regulated by acceptable use statements that a user consents to when using the network
- staff members are not permitted to install software on a School-owned devices without the consent of the SLT/IT department.
- removable media is not permitted unless approved by the SLT/IT department.
- systems are in place to control and protect personal data and data is encrypted at rest and in transit.
- mobile device security and management procedures are in place through our Mobile Device Management Policy
- guest users are provided with appropriate access to School systems based on an identified risk profile.

Mobile technologies

The DfE guidance "Keeping Children Safe in Education" states:
The School or college should have a clear policy on the use of mobile and smart technology. Amongst other things this will reflect the fact many children have unlimited and unrestricted access to the internet via mobile phone networks (i.e., 3G, 4G and 5G). This access means some children, whilst at School or college, sexually harass, bully, and control others via their mobile and smart technology, share indecent images consensually and non-consensually (often via large chat groups) and view and share pornography and other harmful content. Schools and colleges should carefully consider how this is managed on their premises and reflect this in their mobile and smart technology policy and their child protection policy.

Mobile technology devices may be School owned/provided or personally owned and might include smartphone, tablet, wearable devices, notebook/laptop or other technology that usually has the capability of utilising the School's wireless network. The device then has access to the wider internet which may include the School learning platform and other cloud-based services such as e-mail and data storage.

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

We are 'smart phone free' in Fourths and Removes, rolling through to Fifths from September 2027. We are currently reviewing our approach to the management of specialist devices.

The School acceptable use agreements for staff, pupils, parents, and guardians outline the expectations around the use of mobile technologies.

The School allows:

	School devices			Personal devices		
	School owned for individual use	School owned for multiple users	Authorised device[1]	Student owned	Staff owned	Visitor owned
Allowed in School	**X**	**X**	**X**	X	X	X
Full network access	X	X	X	X	X	
Internet only						
No network access						X

School owned/provided devices:

- there is an asset log that clearly states whom a device has been allocated to. There is clear guidance on where, when and how use is allowed
- any designated mobile-free zone is clearly signposted
- personal use (e.g., online banking, shopping, images etc.) is clearly defined and expectations are well-communicated.
- the use of devices on trips/events away from School is clearly defined and expectation are well-communicated.
- liability for damage aligns with current School policy for the replacement of equipment.
- education is in place to support responsible use.

Personal devices:

- there is a clear policy covering the use of personal mobile devices on School premises for all users
- where devices are used to support learning, staff have been trained in their planning, use and implementation, ensuring that all pupils can access a required resource.
- where personal devices are brought to School, but their use is not permitted, appropriate, safe and secure storge should be made available.
- use of personal devices for School business is defined in the acceptable use policy and staff handbook. Personal devices commissioned onto the School network are segregated effectively from School-owned systems
- the expectations for taking/storing/using images/video aligns with the School's acceptable use policy and use of images/video policy. The non-consensual taking/using of images of others is not permitted.
- liability for loss/damage or malfunction of personal devices is clearly defined
- there is clear advice and guidance at the point of entry for visitors to acknowledge School requirements
- education about the safe and responsible use of mobile devices is included in the School online safety education programmes

Social media

With widespread use of social media for professional and personal purposes a policy that sets out clear guidance for staff to manage risk and behaviour online is essential. Core messages should include the protection of pupils, the School and the individual when publishing any material online.

Expectations for teachers' professional conduct are set out in the DfE Teachers Standards but all adults working with children and young people must understand that the nature and responsibilities of their work place them in a position of trust and that their conduct should reflect this.

All Schools and local authorities have a duty of care to provide a safe learning environment for pupils and staff. Schools could be held responsible, indirectly for acts of their employees in the course of their employment. Staff members who harass, bully online, discriminate on the grounds of sex, race, or disability or who defame a third party may render the School liable to the injured party. Reasonable steps to prevent predictable harm must be in place.

The School provides the following measures to ensure reasonable steps are in place to minimise risk of harm to pupils through:

- ensuring that personal information is not published.
- education/training being provided including acceptable use, age restrictions, social media risks, digital and video images policy, checking of settings, data protection and reporting issues.
- clear reporting guidance, including responsibilities, procedures, and sanctions.
- risk assessment, including legal risk.
- guidance for pupils, parents/guardians

School staff should ensure that:

- No reference is made in social media to pupils, parents/guardians or School staff on personal accounts.
- they do not engage in online discussion on personal matters relating to members of the School community.
- personal opinions are not be attributed to the School.
- security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.
- they act as positive role models in their use of social media

When official School social media accounts are established, there are:

- a process for approval by senior leaders
- clear processes for the administration, moderation, and monitoring of these accounts – involving at least two members of staff
- a code of behaviour for users of the accounts
- systems for reporting and dealing with abuse and misuse
- understanding of how incidents may be dealt with under School disciplinary procedures.

Personal use

- personal communications are those made via personal social media accounts. In all cases, where a personal account is used which associates itself with, or impacts on, the School it must be made clear that the member of staff is not communicating on behalf of the School with an appropriate disclaimer. Such personal communications are within the scope of this policy

- personal communications which do not refer to or impact upon the School are outside the scope of this policy
- where excessive personal use of social media in School is suspected, and considered to be interfering with relevant duties, disciplinary action may be taken
- the School permits reasonable and appropriate access to personal social media sites during School hours

Monitoring of public social media

- As part of active social media engagement, the School may pro-actively monitor the Internet for public postings about the School
- the School should effectively respond to social media comments made by others according to a defined policy or process
- when parents/guardians express concerns about the School on social media we will urge them to make direct contact with the School, in private, to resolve the matter. Where this cannot be resolved, parents/guardians should be informed of the School complaints procedure

School use of social media for professional purposes will be checked regularly by the DSL to ensure compliance with the social media, data protection, communications, digital image and video policies. In the event of any social media issues that the School is unable to resolve support may be sought from the Professionals Online Safety Helpline.

Digital and video images

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

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

- the School may use live-streaming or video-conferencing services in line with national and local safeguarding guidance / policies and adopts guidance on the SWGfL Safer Remote Learning web pages and in the DfE Safeguarding and remote education
- when using digital images, staff will inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images
- staff/volunteers must be aware of those pupils whose images must not be taken/published. Those images should only be taken on School devices. The personal devices of staff should not be used for such purposes
- in accordance with guidance from the Information Commissioner's Office, parents/guardians are welcome to take videos and digital images of their children at School events for their own personal use (as such use in not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published/made publicly available on social networking sites, nor should parents/guardians comment on any activities involving other pupils in the digital/video images

- staff and volunteers are allowed to take digital/video images to support educational aims, but must follow School policies concerning the sharing, storage, distribution and publication of those images
- care should be taken when sharing digital/video images that pupils are appropriately dressed
- pupils must not take, use, share, publish or distribute images of others without their permission
- photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with Online Safety Policy
- pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs
- permission for the capture and use of digital images and audio-visual recordings is granted via the Parent Contract. The School's Privacy Notice contains further detail about the purpose, storage, retention and rights around personal data, including digital images and vision.

Online Publishing

The School communicates with parents/guardians and the wider community and promotes the School through:

- Public-facing website
- Social media
- Online newsletters

The School website is managed by the School marketing department and is hosted Finalsite. The School ensures that online safety policy has been followed in the use of online publishing e.g., use of digital and video images, copyright, identification of young people, publication of School calendars and personal information – ensuring that there is least risk to members of the School community, through such publications.

Where learner work, images or videos are published, their identities are protected, and full names are not published.

The School provides information about online safety; curating latest advice and guidance; news articles etc.

Outcomes

The impact of the Online Safety Policy and practice is regularly evaluated through the review/audit of online safety incident logs; behaviour/bullying reports; surveys of staff, pupils; parents/guardians and is reported to relevant groups:

- there is balanced professional debate about the evidence taken from the reviews/audits and the impact of preventative work e.g., online safety education, awareness, and training
- there are well-established routes to regularly report patterns of online safety incidents and outcomes to School leadership and Governors
- parents/guardians are informed of patterns of online safety incidents as part of the School's online safety awareness raising
- online safety (and related) policies and procedures are regularly updated in response to the evidence gathered from these reviews/audits/professional debate
- the evidence of impact is shared with other Schools, agencies and LAs to help ensure the development of a consistent and effective local online safety strategy.

Charterhouse would like to acknowledge SWGFL whose policies, documents, advice and guidance have contributed to the development of this School Online Safety Policy and acknowledge that every effort has been made to ensure that the information included in this document is accurate.

Related Policies

- Pupil Acceptable Use Agreement
- Mobile Device Management Policy
- Social Media Policy Staff and Pupils (to include Staff Acceptable Use Policy)
- AI Policy

Legislation

Schools should be aware of the legislative framework under which this online safety policy and guidance has been produced. It is important to note that in general terms an action that is illegal if committed offline is also illegal if committed online.

It is recommended that legal advice is sought in the advent of an online safety issue or situation.

A useful summary of relevant legislation can be found at: Report Harmful Content: Laws about harmful behaviours

Computer Misuse Act 1990

This Act makes it an offence to:

- Erase or amend data or programs without authority;
- Obtain unauthorised access to a computer;
    - "Eavesdrop" on a computer;
- Make unauthorised use of computer time or facilities;
- Maliciously corrupt or erase data or programs;
- Deny access to authorised users.

Schools may wish to view the National Crime Agency website which includes information about "Cyber crime – preventing young people from getting involved". Each region in England (& Wales) has a Regional Organised Crime Unit (ROCU) Cyber-Prevent team that works with Schools to encourage young people to make positive use of their cyber skills. There is a useful summary of the Act on the NCA site.

Data Protection Act 1998

This protects the rights and privacy of individual's data. To comply with the law, information about individuals must be collected and used fairly, stored safely and securely and not disclosed to any third party unlawfully. The Act states that person data must be:

- Fairly and lawfully processed.
- Processed for limited purposes.
- Adequate, relevant and not excessive.
    - Accurate.
- Not kept longer than necessary.
- Processed in accordance with the data subject's rights.
- Secure.
- Not transferred to other countries without adequate protection.

The Data Protection Act 2018:

Updates the 1998 Act, incorporates the General Data Protection Regulations (GDPR) and aims to:

- Facilitate the secure transfer of information within the European Union.
- Prevent people or organisations from holding and using inaccurate information on individuals. This applies to information regarding both private lives or business.
- Give the public confidence about how businesses can use their personal information.

- Provide data subjects with the legal right to check the information businesses hold about them. They can also request for the data controller to destroy it.
- Give data subjects greater control over how data controllers handle their data.
- Place emphasis on accountability. This requires businesses to have processes in place that demonstrate how they're securely handling data.
- Require firms to keep people's personal data safe and secure. Data controllers must ensure that it is not misused.
- Require the data user or holder to register with the Information Commissioner.

All data subjects have the right to:

- Receive clear information about what you will use their data for.
- Access their own personal information.
- Request for their data to be revised if out of date or erased. These are known as the right to rectification and the right to erasure
- Request information about the reasoning behind any automated decisions, such as if computer software denies them access to a loan.
    - Prevent or query about the automated processing of their personal data.

Freedom of Information Act 2000

The Freedom of Information Act gives individuals the right to request information held by public authorities. All public authorities and companies wholly owned by public authorities have obligations under the Freedom of Information Act. When responding to requests, they have to follow a number of set procedures.

Communications Act 2003

Sending by means of the Internet a message or other matter that is grossly offensive or of an indecent, obscene or menacing character; or sending a false message by means of or persistently making use of the Internet for the purpose of causing annoyance, inconvenience or needless anxiety is guilty of an offence liable, on conviction, to imprisonment. This wording is important because an offence is complete as soon as the message has been sent: there is no need to prove any intent or purpose.

Malicious Communications Act 1988

It is an offence to send an indecent, offensive, or threatening letter, electronic communication or other article to another person.

Regulation of Investigatory Powers Act 2000

It is an offence for any person to intentionally and without lawful authority intercept any communication. Monitoring or keeping a record of any form of electronic communications is permitted, in order to:

- Establish the facts;
    - Ascertain compliance with regulatory or self-regulatory practices or procedures;
- Demonstrate standards, which are or ought to be achieved by persons using the system;
- Investigate or detect unauthorised use of the communications system;
- Prevent or detect crime or in the interests of national security;
- Ensure the effective operation of the system.
    - Monitoring but not recording is also permissible in order to:
- Ascertain whether the communication is business or personal;
- Protect or support help line staff.
- The School reserves the right to monitor its systems and communications in line with its rights under this act.

Trade Marks Act 1994

This provides protection for Registered Trade Marks, which can be any symbol (words, shapes or images) that are associated with a particular set of goods or services. Registered Trade Marks must not be used without permission. This can also arise from using a Mark that is confusingly similar to an existing Mark.

Copyright, Designs and Patents Act 1988

It is an offence to copy all, or a substantial part of a copyright work. There are, however, certain limited user permissions, such as fair dealing, which means under certain circumstances permission is not needed to copy small amounts for non-commercial research or private study. The Act also provides for Moral Rights, whereby authors can sue if their name is not included in a work they wrote, or if the work has been amended in such a way as to impugn their reputation. Copyright covers materials in print and electronic form, and includes words, images, and sounds, moving images, TV broadcasts and other media (e.g. YouTube).

Telecommunications Act 1984

It is an offence to send a message or other matter that is grossly offensive or of an indecent, obscene or menacing character. It is also an offence to send a message that is intended to cause annoyance, inconvenience or needless anxiety to another that the sender knows to be false.

Criminal Justice & Public Order Act 1994

This defines a criminal offence of intentional harassment, which covers all forms of harassment, including sexual. A person is guilty of an offence if, with intent to cause a person harassment, alarm or distress, they:

- Use threatening, abusive or insulting words or behaviour, or disorderly behaviour; or
- Display any writing, sign or other visible representation, which is threatening, abusive or insulting, thereby causing that or another person harassment, alarm or distress.

Racial and Religious Hatred Act 2006

This Act makes it a criminal offence to threaten people because of their faith, or to stir up religious hatred by displaying, publishing or distributing written material which is threatening. Other laws already protect people from threats based on their race, nationality or ethnic background.

Protection from Harassment Act 1997

A person must not pursue a course of conduct, which amounts to harassment of another, and which he knows or ought to know amounts to harassment of the other. A person whose course of conduct causes another to fear, on at least two occasions, that violence will be used against him is guilty of an offence if he knows or ought to know that his course of conduct will cause the other so to fear on each of those occasions.

Protection of Children Act 1978

It is an offence to take, permit to be taken, make, possess, show, distribute or advertise indecent images of children in the United Kingdom. A child for these purposes is anyone under the age of 18. Viewing an indecent image of a child on your computer means that you have made a digital image. An image of a child also covers pseudo-photographs (digitally collated or otherwise). A person convicted of such an offence may face up to 10 years in prison

Sexual Offences Act 2003

A grooming offence is committed if you are over 18 and have communicated with a child under 16 at least twice (including by phone or using the Internet) it is an offence to meet them or travel to meet them anywhere in the world with the intention of committing a sexual offence. Causing a child under 16 to watch a sexual act is illegal, including looking at images such as videos, photos or webcams, for your own gratification. It is also an offence for a person in a position of trust to engage in sexual activity with any person under 18, with whom they are in a position of trust. (Typically, teachers, social workers, health

professionals, connexions staff fall in this category of trust). Any sexual intercourse with a child under the age of 13 commits the offence of rape.

Public Order Act 1986

This Act makes it a criminal offence to stir up racial hatred by displaying, publishing or distributing written material which is threatening. Like the Racial and Religious Hatred Act 2006 it also makes the possession of inflammatory material with a view of releasing it a criminal offence. Children, Families and Education Directorate page 38 April 2007.

Obscene Publications Act 1959 and 1964

Publishing an "obscene" article is a criminal offence. Publishing includes electronic transmission.

Human Rights Act 1998

This does not deal with any particular issue specifically or any discrete subject area within the law. It is a type of "higher law", affecting all other laws. In the School context, human rights to be aware of include:

- The right to a fair trial
- The right to respect for private and family life, home and correspondence
- Freedom of thought, conscience and religion
- Freedom of expression
- Freedom of assembly
- Prohibition of discrimination
- The right to education

These rights are not absolute. The School is obliged to respect these rights and freedoms, balancing them against those rights, duties and obligations, which arise from other relevant legislation.

The Education and Inspections Act 2006

Empowers Heads, 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.

The Education and Inspections Act 2011

Extended the powers included in the 2006 Act and gave permission for Heads (and nominated staff) to search for electronic devices. It also provides powers to search for data on those devices and to delete data.

(see template policy in these appendices and for DfE guidance - http://www.education.gov.uk/Schools/learnersupport/behaviour/behaviourpolicies/f0076897/screening-searching-and-confiscation)

The Protection of Freedoms Act 2012

Requires Schools to seek permission from a parent/guardian to use Biometric systems

The School Information Regulations 2012

Requires Schools to publish certain information on its website:

https://www.gov.uk/guidance/what-maintained-Schools-must-publish-online

Serious Crime Act 2015

Introduced new offence of sexual communication with a child. Also created new offences and orders around gang crime (including CSE)

Criminal Justice and Courts Act 2015

Revenge porn – as it is now commonly known – involves the distribution of private and personal explicit images or video footage of an individual without their consent, with the intention of causing them embarrassment and distress. Often revenge porn is used maliciously to shame ex-partners. Revenge porn

was made a specific offence in the Criminal Justice and Courts Act 2015. The Act specifies that if you are accused of revenge porn and found guilty of the criminal offence, you could be prosecuted and face a sentence of up to two years in prison.

For further guidance or support please contact the Revenge Porn Helpline

Links to other organisations or documents

UK Safer Internet Centre

Safer Internet Centre – https://www.saferinternet.org.uk/
South West Grid for Learning - https://swgfl.org.uk/products-services/online-safety/
Childnet – http://www.childnet-int.org/
Professionals Online Safety Helpline - http://www.saferinternet.org.uk/about/helpline
Revenge Porn Helpline - https://revengepornhelpline.org.uk/
Internet Watch Foundation - https://www.iwf.org.uk/
Report Harmful Content - https://reportharmfulcontent.com/
Harmful Sexual Support Service

CEOP

CEOP - http://ceop.police.uk/
ThinkUKnow - https://www.thinkuknow.co.uk/

Others

LGfL – Online Safety Resources
Kent – Online Safety Resources page
INSAFE/Better Internet for Kids - https://www.betterinternetforkids.eu/
UK Council for Internet Safety (UKCIS) - https://www.gov.uk/government/organisations/uk-council-for-internet-safety

Tools for Schools / other organisations

Online Safety BOOST – https://boost.swgfl.org.uk/
360 Degree Safe – Online Safety self-review tool – https://360safe.org.uk/
360Data – online data protection self-review tool: www.360data.org.uk
SWGfL Test filtering - http://testfiltering.com/
UKCIS Digital Resilience Framework - https://www.gov.uk/government/publications/digital-resilience-framework
SWGfL 360 Groups – online safety self review tool for organisations working with children
SWGfL 360 Early Years - online safety self review tool for early years organisations

Bullying/Online-bullying/Sexting/Sexual Harassment

Enable – European Anti Bullying programme and resources (UK coordination/participation through SWGfL & Diana Awards) - http://enable.eun.org/
SELMA – Hacking Hate - https://selma.swgfl.co.uk
Scottish Anti-Bullying Service, Respectme - http://www.respectme.org.uk/
Scottish Government - Better relationships, better learning, better behaviour - http://www.scotland.gov.uk/Publications/2013/03/7388
DfE - Cyberbullying guidance - https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/374850/Cyberbullying_Advice_for_Headteachers_and_School_Staff_121114.pdf
Childnet – Cyberbullying guidance and practical PSHE toolkit: http://www.childnet.com/our-projects/cyberbullying-guidance-and-practical-toolkit
Childnet – Project deSHAME – Online Sexual Harrassment
UKSIC – Sexting Resources
Anti-Bullying Network – http://www.antibullying.net/cyberbullying1.htm
Ditch the Label – Online Bullying Charity
Diana Award – Anti-Bullying Campaign

Social Networking

Digizen – Social Networking
UKSIC - Safety Features on Social Networks

Children's Commissioner, TES and Schillings – Young peoples' rights on social media

Curriculum

SWGfL Evolve - https://projectevolve.co.uk
UKCCIS – Education for a connected world framework
Department for Education: Teaching Online Safety in Schools

Teach Today – www.teachtoday.eu/
Insafe - Education Resources

Data Protection

360data - free questionnaire and data protection self review tool

ICO Guides for Organisations

IRMS - Records Management Toolkit for Schools

ICO Guidance on taking photos in Schools

Professional Standards/Staff Training

DfE – Keeping Children Safe in Education
DfE - Safer Working Practice for Adults who Work with Children and Young People
Childnet – School Pack for Online Safety Awareness
UK Safer Internet Centre Professionals Online Safety Helpline

Infrastructure/Technical Support/Cyber-security

UKSIC – Appropriate Filtering and Monitoring
SWGfL Safety & Security Resources
Somerset - Questions for Technical Support
SWGfL - Cyber Security in Schools.
NCA – Guide to the Computer Misuse Act
NEN – Advice and Guidance Notes

Working with parents and guardians

SWGfL – Online Safety Guidance for Parents & Guardians
Vodafone Digital Parents Magazine
Childnet Webpages for Parents & Guardians
Get Safe Online - resources for parents
Teach Today - resources for parents workshops/education
Internet Matters

Prevent

Prevent Duty Guidance
Prevent for Schools – teaching resources
Childnet – Trust Me

Research

Ofcom –Media Literacy Research
Ofsted: Review of sexual abuse in Schools and colleges

Further links can be found at the end of the UKCIS Education for a Connected World Framework

Glossary of Terms

AUP/AUA	Acceptable Use Policy/Agreement – see templates earlier in this document
CEOP	Child Exploitation and Online Protection Centre (part of National Crime Agency, UK Police, dedicated to protecting children from sexual abuse, providers of the Think U Know programmes.
CPD	Continuous Professional Development
FOSI	Family Online Safety Institute

ICO	Information Commissioners Office
ICT	Information and Communications Technology
INSET	In Service Education and Training
IP address	The label that identifies each computer to other computers using the IP (internet protocol)
ISP	Internet Service Provider
ISPA	Internet Service Providers' Association
IWF	Internet Watch Foundation
LA	Local Authority
LAN	Local Area Network
MAT	Multi Academy Trust
MIS	Management Information System
NEN	National Education Network – works with the Regional Broadband Consortia (e.g. SWGfL) to provide the safe broadband provision to Schools across Britain.
Ofcom	Office of Communications (Independent communications sector regulator)
SWGfL	South West Grid for Learning Trust – the Regional Broadband Consortium of SW Local Authorities – is the provider of broadband and other services for Schools and other organisations in the SW
TUK	Think U Know – educational online safety programmes for Schools, young people and parents.
UKSIC	UK Safer Internet Centre – EU funded centre. Main partners are SWGfL, Childnet and Internet Watch Foundation.
UKCIS	UK Council for Internet Safety
VLE	Virtual Learning Environment (a software system designed to support teaching and learning in an educational setting,
WAP	Wireless Application Protocol

A more comprehensive glossary can be found at the end of the UKCIS Education for a Connected World Framework