STONAR

Stonar School

Online Safety Policy

(Including EYFS)

Policy agreed by the Proprietors' Board of Directors:	May 2024
Next review:	May 2025
Policy owner:	Deputy Head, Pastoral/DSL

TABLE OF CONTENTS

1. Scope of the Online Safety Policy

This policy applies to all members of the school community (including staff, pupils, volunteers, parents and carers, 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).

The Policy outlines the commitment of Stonar School to safeguard members of our school community online in accordance with statutory guidance and best practice. The policy should also be read in conjunction with the Safeguarding Policy, Data Protection Policy, Behaviour and Discipline Policy (including EYFS), Whole School Policy for Dealing with Conflicts and with the Code of Conduct for Staff.

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

The School Online Safety Policy:

i. Sets expectations for the safe and responsible use of digital technologies for learning, administration, and communication.
ii. Allocates responsibilities for the delivery of the policy.
iii. Is regularly reviewed in a collaborative manner, taking account of online safety incidents and changes/trends in technology and related behaviours.
iv. 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.
v. Describes how the School will help prepare pupils to be safe and responsible users of online technologies.
vi. Establishes clear procedures to identify, report, respond to and record the misuse of digital technologies and online safety incidents, including external support mechanisms.
vii. Is supplemented by a series of related Acceptable Use Agreements (AUAs).
viii. Is made available to staff at induction and through normal communication channels.
ix. Is published on the school website.

2. Policy Development, Monitoring and Review

This Online Safety Policy has been developed by the Designated Safeguarding Lead (DSL) and Online Safety Officers made up of:

Tina Tilley	Deputy Head (Pastoral) & DSL
James Cole	Subject lead computer Science
Dan Gower	Deputy Head Prep School and Co-Curricular lead
Tom Kamm	IT Technician

Consultation with the whole school community has taken place through a range of formal and informal meetings.

3. Schedule for Development, Monitoring and Review

This Online Safety Policy was approved by the Proprietor's Board of Directors (Governors) at the Advisory Board meeting:	16 May 2024
The implementation of this Online Safety Policy will be monitored by:	DSL & Online Safety Officers
Monitoring will take place at regular intervals:	Termly
The Proprietors Board of Directors (Governors) 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
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:	01/05/25
Should serious online safety incidents take place, the following external persons/agencies should be informed:	Headmaster, Designated Safeguarding Lead and Nominated Safeguarding Proprietors Board of Directors (Governors). They will determine the course of action to be taken. If the issue involves safeguarding concerns, then the School's Safeguarding policy will be followed in order to determine whether to inform external persons/agencies.

4. Process for Monitoring the Impact of the Online Safety Policy

The School will monitor the impact of the policy using:

i. Logs of reported incidents
ii. Filtering and monitoring logs
iii. Internal monitoring data for network activity

5. 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.

5.1 Headmaster and Executive Management Group (EMG)

i. The Headmaster 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 DSL, as defined in Keeping Children Safe in Education.
ii. The Headmaster and (at least) another member of the Executive Management Group (EMG) 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.
iii. The Headmaster and EMG are responsible for ensuring that the DSL/Online Safety Lead (OSL), IT provider/technical staff, and other relevant staff carry out their responsibilities effectively and receive suitable training to enable them to carry out their roles and train other colleagues, as relevant.
iv. The Headmaster and EMG 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.
v. The Headmaster and EMG will receive regular monitoring reports from the DSL/OSL.
vi. The Headmaster and EMG will work with the responsible Advisory Board Member, the DSL and IT service providers in all aspects of filtering and monitoring.

5.2 Proprietors Board of Directors (Governors)

The Board of Proprietors Directors are responsible for the approval of the Online Safety Policy and for reviewing the effectiveness of the policy. They are advised by the advisory Board. The Board of Proprietors Directors will receive regular information about online

safety incidents and monitoring reports. Kath Tyler is Proprietor representative responsible for Online Safety at Stonar and her will role will include:

i. Termly meetings with the DSL/OSL.
ii. Receiving (collated and anonymised) reports of online safety incidents termly.
iii. Checking that provision outlined in the Online Safety Policy (e.g. online safety education provision and staff training is taking place as intended).
iv. Ensuring that the filtering and monitoring provision is reviewed and recorded, at least annually.
v. Reporting to relevant Board of Proprietors Directors and Advisory Board.
vi. Receiving (at least) basic cyber-security training to enable the Board of Proprietors Directors and Advisory Board to check that the School meets the DfE Cyber-Security Standards.

The Board of Proprietors Directors will also support the School in encouraging parents/carers and the wider community to become engaged in online safety activities.

5.3 Designated Safety Lead (DSL)

The DSL will:

i. Hold the lead responsibility for online safety, within their safeguarding role.
ii. 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.
iii. Meet regularly with the Proprietor representative responsible for Online Safety at Stonar to discuss current issues, review (anonymised) incidents and filtering and monitoring logs and ensure that annual (at least) filtering and monitoring checks are carried out.
iv. Attend relevant Board of Proprietors Directors and advisory body meetings.
v. Report regularly to Headmaster/EMG
vi. 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.
vii. Liaise with staff and IT providers on matters of safety and safeguarding and welfare (including online and digital safety)

5.4 Online Safety Lead

The OSL will:

i. Lead the Online Safety Group.

ii. 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.
iii. Have a leading role in establishing and reviewing the school online safety policies/documents.
iv. Promote an awareness of and commitment to online safety education / awareness raising across the school and beyond.
v. Liaise with curriculum leaders to ensure that the online safety curriculum is planned, mapped, embedded and evaluated.
vi. 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.
vii. Provide (or identify sources of) training and advice for staff/ Board of Proprietors Directors /parents/carers /learners.
viii. Liaise with (school/local authority/MASH external provider) technical staff, pastoral staff and support staff (as relevant).
ix. Receive regularly updated training to allow them to understand how digital technologies are used and are developing (particularly by pupils) with regard to the areas defined in Keeping Children Safe in Education:

a) Content
b) Contact
c) Conduct
d) Commerce

5.5 Curriculum Leads

Curriculum Leads will work with the DSL/OSL to develop a planned and coordinated online safety education programme.

This will be provided through:

i. A discrete programme
ii. PHSEE and SRE programmes
iii. A mapped cross-curricular programme
iv. Assemblies and pastoral programmes
v. Through relevant national initiatives and opportunities e.g. Safer Internet Day and Anti-bullying week.

5.6 Teaching and Support Staff

School staff are responsible for ensuring that:

i. They have an awareness of current online safety matters/trends and of the current school Online Safety Policy and practices.

ii. They understand that online safety is a core part of safeguarding.
iii. They have read, understood, and signed the staff AUA.
iv. They immediately report any suspected misuse or problem to a member of the safeguarding team for investigation/action, in line with the school safeguarding procedures.
v. All digital communications with pupils and parents/carers are on a professional level and only carried out using official school systems.
vi. Online safety issues are embedded in all aspects of the curriculum and other activities.
vii. Ensure pupils understand and follow the Online Safety Policy and AUAs, have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.
viii. 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.
ix. In lessons where internet use is pre-planned learners 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
x. Where lessons take place using live-streaming or videoconferencing, there is regard to national safeguarding guidance and local safeguarding policies.
xi. There is a zero-tolerance approach to incidents of online-bullying, sexual harassment, discrimination, hatred etc.
xii. 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.

5.7 IT Provider

If the School has a technology service provided by an outside contractor, it is the responsibility of the school to ensure that the provider carries out all the online safety measures that the school's obligations and responsibilities require. It is also important that the provider follows and implements school Online Safety Policy and procedures.

The IT Provider is responsible for ensuring that:

i. They are aware of and follow the school Online Safety Policy and Technical Security Policy to carry out their work effectively in line with school policy.
ii. The school technical infrastructure is secure and is not open to misuse or malicious attack.
iii. 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 / MASH or other relevant body
iv. There is clear, safe, and managed control of user access to networks and devices.
v. They keep up to date with online safety technical information in order to effectively carry out their online safety role and to inform and update others as relevant.

vi. The use of technology is regularly and effectively monitored in order that any misuse/attempted misuse can be reported to DSL for investigation and action. This must be reported in person or via email.
vii. The filtering policy is applied and updated on a regular basis and its implementation is not the sole responsibility of any single person.
viii. Monitoring systems are implemented and regularly updated as agreed in school policies.

5.8 Pupils

i. Are responsible for using the school digital technology systems in accordance with the pupil AUA and Online Safety Policy.
ii. Should understand the importance of reporting abuse, misuse or access to inappropriate materials and know to report to the DSL in person or via email or via their trusted adult immediately. Out of hours boarders can report to their Houseparent/Assistant Houseparent and ask for them to contact the member of SLT on call duty.
iii. Pupils know to report to the DSL in person or via email or via their trusted adult if they or someone they know feels vulnerable when using online technology. Out of hours boarders can report to their Houseparent/Assistant Houseparent and ask for them to contact the member of SLT on call duty.
iv. 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.

5.9 Parents and Carers

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

i. Publishing the school Online Safety Policy on the school website
ii. Providing them with a copy of the pupils' AUA
iii. Publish information about appropriate use of social media relating to posts concerning the school.
iv. Seeking their permissions concerning digital images, cloud services etc
v. Parents'/carers' evenings, newsletters, website, social media and information about national/local online safety campaigns and literature.
vi. Parents and carers will be encouraged to support the school in:

vii. Reinforcing the online safety messages provided to learners in school.
viii. The safe and responsible use of their children's personal devices in the school (where this is allowed)

5.10 Community Users

Community users who access School systems/website/learning platform as part of the wider school provision will be expected to sign a community user AUA before being provided with access to school systems.

6. Online Safety Group

The Online Safety Group has the following members:

i. Tina Tilley - Deputy Head (Pastoral) & DSL
ii. James Cole – Subject lead Computer Science/ Online Safety Officer
iii. Dan Gower - Deputy Head Prep School and Co-Curricular lead/ Online Safety Officer
iv. Tom Kamm - IT Technician// Online Safety Officer

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

i. The production/review/monitoring of the school Online Safety Policy/documents.
ii. The production/review/monitoring of the school filtering policy and requests for filtering changes.
iii. Mapping and reviewing the online safety education provision – ensuring relevance, breadth and progression and coverage.
iv. Reviewing network/filtering/monitoring/incident logs, where possible.
v. Encouraging the contribution of learners to staff awareness, emerging trends and the school online safety provision.
vi. Consulting stakeholders – including staff/parents/carers about the online safety provision.
vii. Monitoring improvement actions identified through use of the 360-degree safe self-review tool.

An Online Safety Group terms of reference template can be found in the appendices.

7. 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.

8. Online Safety Policy Agreement

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

8.1 Training and Awareness of the Terms of the Agreements

The online safety policy and AUA define acceptable use at the school. The online safety policy and the AUA will be communicated/re-enforced through:

i. Pupil induction and joining pack
ii. Staff induction and handbook
iii. Splash screens
iv. Digital signage
v. Posters/notices around where technology is used.
vi. Communication with parents/carers
vii. Built into education sessions.
viii. School website
ix. Peer support.

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

User Actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
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					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	

	Staff and other adults				Pupils			
Consideration should be given for the following activities when undertaken for non-educational purposes: Schools may wish to add further activities to this list.	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 (Out of sight) (Not in EYFS setting				x (Age related – see device policy)	
Use of mobile phones for learning at school	X							X (Age related – see device policy)
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			

9. Good Practice

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

i. When communicating in a professional capacity, staff should ensure that the technologies they use are officially sanctioned by the school.
ii. 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.
iii. 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.
iv. 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.
v. 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.

10. Reporting and Responding

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

i. 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.
ii. All members of the school community will be made aware of the need to report online safety issues/incidents. Pupils should report any suspicious or inappropriate sexual advances, messages or similar online behaviour to their parent, houseparent or teacher; they may also report serious or urgent suspicions to the police by using the CEOP button available on many online chat & social networking sites or seek help via the CEOP website.
Staff should report any concerns to a member of the Leadership Team and safeguarding concerns to the Designated Safeguarding Lead for Child Protection or in their absence a member of the Stonar Safeguarding Team.
iii. Reports will be dealt with as soon as is practically possible once they are received.
iv. The DSL/OSL and other responsible staff have appropriate skills and training to deal with online safety risks.
v. If there is any suspicion that the incident involves any illegal activity or the potential for serious harm, the incident must be escalated through the agreed school safeguarding procedures, this may include.
    a) Non-consensual images
    b) Self-generated images
    c) Terrorism/extremism
    d) Hate crime/ Abuse.
    e) Fraud and extortion
    f) Harassment/stalking
    g) Child Sexual Abuse Material (CSAM)
    h) Child Sexual Exploitation Grooming
    i) Extreme Pornography
    j) Sale of illegal materials/substances
    k) Cyber or hacking
    l) Copyright theft or piracy

vi. Any concern about staff misuse will be reported to the Headmaster, unless the concern involves the Headmaster, in which case the complaint is referred to the Director Daniel Jones and the local authority/MASH.
vii. Where there is no suspected illegal activity, devices may be checked using the following procedures:
    a) One or more senior members of staff should be involved in this process. This is vital to protect individuals if accusations are subsequently reported.
    b) Conduct the procedure using a designated device that will not be used by learners and, if necessary, can be taken off site by the police should the need arise (should illegal activity be subsequently suspected). Use the same device for the duration of the procedure.
    c) 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).
    d) 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.

e) Once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does, then appropriate action will be required and could include the following:
   - internal response or discipline procedures
   - involvement by local authority / MASH (as relevant)
   - police involvement and/or action

viii. It is important that those reporting an online safety incident have confidence that the report will be treated seriously and dealt with effectively.

ix. There are support strategies in place e.g., peer support for those reporting or affected by an online safety incident.

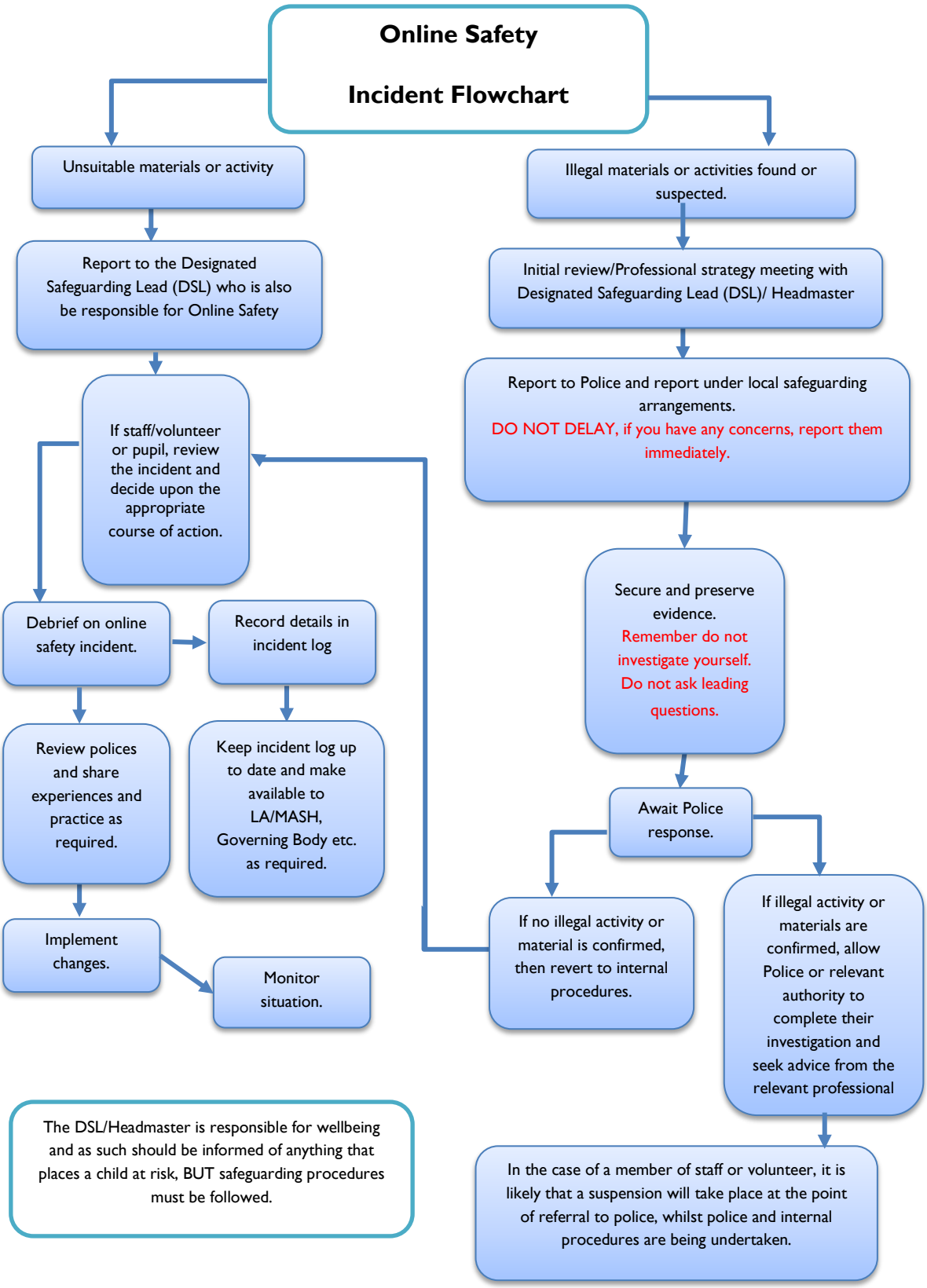
x. Incidents should be logged.

xi. Relevant staff are aware of external sources of support and guidance in dealing with online safety issues, e.g. local authority; police.

xii. Those involved in the incident will be provided with feedback about the outcome of the investigation and follow up actions.

xiii. Learning from the incident (or pattern of incidents) will be provided to:
   a) The Online Safety Group for consideration of updates to policies or education programmes and to review how effectively the report was dealt with.
   b) Staff, through regular briefings
   c) Pupils, through assemblies/lessons
   d) Parents/carers, through newsletters, school social media, website
   e) Directors of Proprietors, through regular safeguarding updates
   f) Local authority/external agencies, as relevant

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


Online Safety
Incident Flowchart
Unsuitable materials or activity
Report to the Designated Safeguarding Lead (DSL) who is also be responsible for Online Safety
If staff/volunteer or pupil, review the incident and decide upon the appropriate course of action.
Debrief on online safety incident.
Record details in incident log
Review polices and share experiences and practice as required.
Keep incident log up to date and make available to LA/MASH, Governing Body etc. as required.
Implement changes.
Monitor situation.
Illegal materials or activities found or suspected.
Initial review/Professional strategy meeting with Designated Safeguarding Lead (DSL)/ Headmaster
Report to Police and report under local safeguarding arrangements.
DO NOT DELAY, if you have any concerns, report them immediately.
Secure and preserve evidence.
Remember do not investigate yourself.
Do not ask leading questions.
Await Police response.
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
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.
The DSL/Headmaster is responsible for wellbeing and as such should be informed of anything that places a child at risk, BUT safeguarding procedures must be followed.

11. 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:

11.1 Responding to Pupils' Actions

Incidents	DSL/Head to inform the class teacher (Prep)/tutor or Mentor (Senior)	Refer to DSL (safeguarding Team)	Refer to /inform Head	Refer to Police/Social Work	Refer to local authority technical support for advice/action	Inform parents/carers	Remove device/ network/internet access rights	Further sanction, in line with behaviour policy
Deliberately accessing or trying to access material that could be considered illegal.	X	X	X	X	X	X	X	X
Attempting to access or accessing the school network, using another user's account (staff or pupil) or allowing others to access school network by sharing username and passwords	X (Pupil)	X (Pupil)	X (Pupil/ Staff)	(X) (Dep-ending on actions)		X (pupil)	X	X
Corrupting or destroying the data of other users.	X	X	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	X (Dep-ending on seriousness)	X (Dep-ending on seriousness)	X	X	X
Unauthorised downloading or uploading of files or use of file sharing.	X	X	X			X	X	X
Using proxy sites, virtual private networks (VPNs) or other means to subvert the school's filtering system.	X	X				X	X	X
Accidentally accessing offensive or pornographic material and failing to report the incident.	X	X	X			X	X	X

Deliberately accessing or trying to access offensive or pornographic material.	X	X	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)		X	X	X
Unauthorised use of digital devices (including taking images)	X	X	X	(X)	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			X	X	X
Continued infringements of the above, following previous warnings or sanctions.	X	X	X			X	X	X

11.2 Responding to Staff Actions

Incidents	Refer to line manager	Refer to Head	Refer to local authority/MAT/HR	Refer to Police	Refer to 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	X	X
Deliberate actions to breach data protection or network security rules.		X			X	X	X	X
Deliberately accessing or trying to access offensive or pornographic material.		X	X	(X)	X		X	X
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software.		X			X		X	X
Using proxy sites, virtual personal networks (VPNs) or other means to subvert the school's filtering system.		X			X			X
Unauthorised downloading or uploading of files or file sharing.		X			X	X		
Breaching copyright or licensing regulations.		X			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	X	X			X	X
Using personal e-mail/social networking/messaging to carry out digital communications with learners and parents/carers.		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	X		
Actions which could compromise the staff member's professional standing.		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

12. Online Safety Education Programme

Keeping Children Safe in Education states that 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:

i. 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.
ii. Lessons are matched to need; are age-related and build on prior learning.
iii. Lessons are context-relevant with agreed objectives leading to clear and evidenced outcomes.
iv. Pupil need and progress are addressed through effective planning and assessment
v. Digital competency is planned and effectively threaded through the appropriate digital pillars in other curriculum areas e.g. PHSEE; SRE; Literacy etc.
vi. It incorporates/makes use of relevant national initiatives and opportunities e.g. Safer Internet Day and Anti-bullying week
vii. 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.
viii. Vulnerability is actively addressed as part of a personalised online safety curriculum e.g., for victims of abuse and SEND.
ix. 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.
x. Staff should act as good role models in their use of digital technologies the internet and mobile devices.
xi. 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.
xii. 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.
xiii. It is accepted that from time to time, for good educational reasons, pupils 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 to the DSL 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.
xiv. The online safety education programme should be relevant and up to date to ensure the quality of learning and outcomes.

12.1 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:

i. Mechanisms to canvass pupil feedback and opinion to include through the Schools Digital Leaders, pupil questionnaires, School Council meetings and discussions during tutor time and curriculum time.
ii. Appointment of leaders e.g. digital leaders
iii. The Online Safety Group has pupil representation.
iv. Pupils contribute to the online safety education programme e.g. peer education, digital leaders leading lessons for younger learners, online safety campaigns.
v. Pupils designing/updating AUAs.
vi. Contributing to online safety events with the wider school community e.g. parents' evenings, family learning programmes etc.

12.2 Staff/Volunteers

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

i. 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.
ii. The training will be an integral part of the school's annual safeguarding and data protection training for all staff.
iii. 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 AUAs. It includes explicit reference to classroom management, professional conduct, online reputation and the need to model positive online behaviours.
iv. The DSL/OSL and online safety officers will receive regular updates through attendance at external training events, (e.g. UKSIC / SWGfL / MASH / LA / other relevant organisations) and by reviewing guidance documents released by relevant organisations.
v. This Online Safety Policy and its updates will be presented to and discussed by staff in staff/team meetings/INSET days.
vi. The DSL/OSL will provide advice/guidance/training to individuals as required.

12.3 Proprietors Board of Directors (Governors)

Proprietors will ensure they have 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:

i. Attendance at training provided by the local authority/MASH or other relevant organisation.
ii. Participation in school training / information sessions for staff or parents

A higher level of training will be made available to (at least) the Proprietor representative responsible for Online Safety at Stonar.

This will include:

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

12.4 Families

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

i. Regular communication, awareness-raising and engagement on online safety issues, curriculum activities and reporting routes
ii. Regular opportunities for engagement with parents/carers on online safety issues through awareness workshops / parent/carer evenings etc
iii. 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/carer evenings.
iv. Letters, newsletters, website, learning platform,
v. High profile events / campaigns e.g. Safer Internet Day
vi. Reference to the relevant web sites/publications, e.g. SWGfL; www.saferinternet.org.uk/; www.childnet.com/parents-and-carers (see Appendix 10 for further links/resources).
vii. Sharing good practice with other schools in clusters and or the local authority/MASH

13. Technology

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.

13.1 Filtering & Monitoring

The School filtering and monitoring provision is agreed by EMG, Proprietors and the IT Service Provider 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 the safeguarding team and IT staff to be effective. The DSL will have lead responsibility for safeguarding and online safety and the IT Manager and IT Technician will have technical responsibility.

The filtering and monitoring provision is reviewed by EMG and, the Designated Safeguarding Lead and a Proprietor with the involvement of the IT Service Provider.

Checks on the filtering and monitoring system are carried out by the IT Service Provider with the involvement of a EMG member, the DSL and a proprieter, in particular when a safeguarding risk is identified, there is a change in working practice, e.g. remote access or BYOD or new technology is introduced for example using the SWGFL Test Filtering.

13.1.1 Filtering

i. The School manages access to content across its systems for all users and on all devices using the school's internet provision, FastVue reporter for Fortigate 600F Firewall. 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.**
ii. 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 by both the DSL and Tom Kamm (Online Safety Officer).
iii. There are established and effective routes for users to report inappropriate content, recognising that no system can be 100% effective.
iv. There is a clear process in place to deal with, and log, requests/approvals for filtering changes. These requests must all go through the DSL.
v. Filtering logs are regularly reviewed and alert the DSL, Head of Prep, IT Manager and Tom Kamm (IT Technician /Online Safety Officer) to breaches of the filtering policy, which are then acted upon immediately.
vi. The school has provided enhanced/differentiated user-level filtering (allowing different filtering levels for different abilities/ages/stages and different groups of users: staff/learners, etc.)
vii. Personal mobile devices have internet access through the school network, content is managed in ways that are consistent with school policy and practice.
viii. 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.

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

13.1.2 Monitoring Systems

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.

The following monitoring systems are in place to protect the school systems and its users:

i. The school monitors all network use across all its devices and services.
ii. Monitoring reports are urgently picked up, acted on and outcomes are recorded by the DSL, all users are aware that the network (and devices) are monitored. The IT Manager and Tom Kamm IT technician/ Online Safety Officer review a minimum of weekly the monitoring reports received from FastVue for Fortigate and alert the DSL to any concerns that need acting upon immediately.
iii. 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.
iv. Management of serious safeguarding alerts is consistent with safeguarding policy and practice.
v. Physical monitoring (adult supervision in the classroom).
vi. Internet use is logged, regularly monitored and reviewed.
vii. Daily filtering logs from FastVue for Fortigate are analysed weekly, and breaches are reported to the DSL and Head of Prep (DDSL).
viii. Pro-active alerts inform the school of breaches to the filtering policy, allowing effective intervention.
ix. Where possible, school technical staff regularly monitor and record the activity of users on the school technical systems.
x. Use of a third-party assisted monitoring service to review monitoring logs and report issues to school monitoring lead(s).
xi. Parents are encouraged to contact school staff if they have any concerns over the use of email or the internet by their child.
xii. The welfare of pupils is of paramount importance; Stonar uses various technologies to monitor both internal and external Internet and e-mail traffic whilst respecting privacy at all times. The School reserves the right to inspect data files and network logs if automatic detection of illicit content is triggered. Manual investigation of email transmissions will only be carried out with the permission of the Head, Deputy Head or Head of Prep.

14. Technical Security

The School technical systems will be managed in ways that ensure that the school meets recommended technical requirements.

i. Responsibility for technical security resides with EMG who may delegate activities to identified roles.
ii. 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 EMG/Online Safety Group
iii. Password policy and procedures are implemented.
iv. The security of their username and password and must not allow other users to access the systems using their log on details.
v. 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.
vi. All school networks and system will be protected by secure passwords. Passwords must not be shared with anyone.
vii. The administrator passwords for school systems are kept in a secure place, e.g. school safe.
viii. There is a risk-based approach to the allocation of pupil usernames and passwords.
ix. There will be regular reviews and audits of the safety and security of school technical systems.
x. Servers, wireless systems and cabling are securely located and physical access restricted.
xi. Appropriate security measures are in 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.
xii. There are rigorous and verified back-up routines, including the keeping of network-separated (air-gapped) copies off-site or in the cloud,
xiii. IT Manager 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.
xiv. An appropriate system is in place for users to report any actual/potential technical incident/security breach to the relevant person, as agreed)
xv. 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.
xvi. Personal use of any device on the school network is regulated by acceptable use statements that a user consents to when using the network.
xvii. Staff members are not permitted to install software on a school-owned devices without the consent of the EMG/IT service provider.
xviii. Removable media is not permitted unless approved by the EMG/IT service provider.
xix. Systems are in place to control and protect personal data and data is encrypted at rest and in transit.

xx. Mobile device security and management procedures are in place.
xxi. Guest users are provided with appropriate access to school systems based on an identified risk profile.

15. Mobile Technologies

The School AUAs for staff, pupils, parents, and carers outline the expectations around the use of mobile technologies.

The School allows:

	School Devices			**Personal Devices (Not in EYFS setting)**		
	School owned for individual use	School owned for multiple users	Authorised device	Pupil owned	Staff owned	Visitor owned
Allowed in school	Yes	Yes	Yes	Yes (Age & time restrictions)	Yes (Need to be out of sight of pupils)	Yes (At certain times)
Full network access	Yes	Yes	Yes	Yes	Yes	No
Internet only	Yes	Yes	Yes	Yes (Age & time restrictions)	Yes	Yes

15.1 School-Owned/Provided Devices

i. All school devices are managed through the use of Mobile Device Management software.
ii. 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.
iii. Any designated mobile-free zone is clearly signposted.
iv. Personal use (e.g. online banking, shopping, images etc.) is clearly defined and expectations are well-communicated.
v. The use of devices on trips/events away from school is clearly defined and expectation are well-communicated.
vi. Liability for damage aligns with current school policy for the replacement of equipment.
vii. Education is in place to support responsible use.

15.2 Personal Devices

i. AUA outlines the use of personal mobile devices on school premises for all users.

ii. 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.
iii. Where personal devices are brought to school, but their use is not permitted, appropriate, safe and secure storage should be made available.
iv. Use of personal devices for school business is defined in the Acceptable Use Policy (AUP) and staff handbook. Personal devices commissioned onto the school network are segregated effectively from school-owned systems.
v. The expectations for taking/storing/using images/video aligns with the school's AUP and use of images/video policy. The non-consensual taking/using of images of others is not permitted.
vi. Liability for loss/damage or malfunction of personal devices is clearly defined.
vii. There is clear advice and guidance at the point of entry for visitors to acknowledge school requirements.
viii. Education about the safe and responsible use of mobile devices is included in the school online safety education programmes.
ix. Prep pupils are not permitted to have mobile devices in school during the school day.
x. Unless directed to by a member of staff, Senior School pupils (Years 7-10) must not use mobile devices during the school day, with the exception that riders are advised to carry a mobile device when they are out hacking or working with horses on fields at some distance from the Equestrian Centre. Senior School pupils (Years 7-10) who choose to bring a mobile device with them to school should secure it in their locker during the school day. Tablets that can access mobile data are not permitted at Stonar.
xi. Pupils in year 11 and Sixth Form are permitted to use their mobile device in the library for work purposes and during break times for personal use in tutor rooms and social spaces.
xii. Boarders (excluding sixth formers) are required to hand in their mobile phones (and other portable devices as requested) to the duty member of boarding staff before bedtime; they can be collected after school (4.05pm) the following day (Year 11 boarders can collect before school at morning roll call). Boarders have access to their mobile devices during the day at weekends.
xiii. The Wi-Fi is turn off in the boarding house overnight for all boarders, the timing of this is age related.
xiv. Mobile devices must never be used in changing rooms or toilets, when moving about the school campus, at the front of school, in corridors, or the dining hall regardless of the time of day / day of the week.
xv. Access to the internet must be via School Wi-Fi. Use of VPN's and 'Hot spotting' is not allowed.

16. Social Media

16.1 Minimising Risk of Harm

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

i. Ensuring that personal information is not published, with the exception of the pupils first name and initial of surname.
ii. Education/training being provided including acceptable use, age restrictions, and social media risks, digital and video images policy, checking of settings, data protection and reporting issues, through the curriculum, in particular in PSHEE and in IT lessons as well as through tutor time and Houseparent regular dialogue with boarders and in Boarding House Meetings. Pupils are educated through guest speaker's in this area.
iii. Clear reporting guidance, including responsibilities, procedures, and sanctions.
iv. Risk assessment, including legal risk.
v. Guidance for pupils, parents/carers

16.2 Responsibilities of School Staff

i. No reference should be made in social media to pupils, parents/carers or school staff.
ii. They do not engage in online discussion on personal matters relating to members of the school community.
iii. Personal opinions should not be attributed to the school.
iv. Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.
v. They act as positive role models in their use of social media.

16.3 Official School Social Media

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

i. A process for approval by EMG
ii. Clear processes for the administration, moderation, and monitoring of these accounts – involving at least two members of staff.
iii. Systems for reporting and dealing with abuse and misuse.
iv. Understanding of how incidents may be dealt with under school disciplinary procedures.

16.4 Personal Use

i. 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.
ii. Personal communications which do not refer to or impact upon the school are outside the scope of this policy.

iii. Where excessive personal use of social media in school is suspected, and considered to be interfering with relevant duties, disciplinary action may be taken.
iv. The school permits reasonable and appropriate access to personal social media sites during school hours.

16.5 Monitoring of Public Social Media

i. As part of active social media engagement, the school pro-actively monitor the Internet for public postings about the school.
ii. The school should effectively respond to social media comments made by others according to a defined policy or process.
iii. When parents/carers 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/carers should be informed of the school complaints procedure.

17. Digital & Video Images

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

i. The School may use live-streaming or video-conferencing services in line with national and local safeguarding guidance / policies.
ii. When using digital images, staff will inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images.
iii. 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.
iv. Parents/carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use in not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published/made publicly available on social networking sites, nor should parents/carers comment on any activities involving other pupils in the digital/video images.
v. Staff and volunteers are allowed to take digital/video images as long as they are using school provided devices to support educational aims, but must follow school policies concerning the sharing, storage, distribution and publication of those images.
vi. Care should be taken when sharing digital/video images that pupils are appropriately dressed.
vii. Photographs published on the website, or elsewhere that include learners will be selected carefully and will comply with Online Safety Policy
viii. Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs.

ix. Permission from parents or carers will be obtained before photographs of pupils are taken for use in school or published on the school website/social media.
x. Parents and Carers will be made aware of the purposes for the use of images, how they will be stored and for how long – in line with the school data protection policy.
xi. Images will be securely stored in line with the school retention policy.
xii. Pupils' work can only be published with the permission of the pupils and parents/carers.

18. Online Publishing

The School communicates with parents/carers and the wider community and promotes the school through.

i. Public-facing website
ii. Social media
iii. Online newsletters

The School website is managed by Sarah Burns Director of Marketing and Admissions 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 pupils work, images or videos are published, their identities are protected, and full names are not published.

19. Data Protection

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

The School:

i. Has a Data Protection Policy.
ii. Implements the data protection principles and can demonstrate that it does so.
iii. Has paid the appropriate fee to the Information Commissioner's Office (ICO)
iv. The Senior Deputy Head oversees the data protection at the school, she has effective understanding of data protection law.
v. Has a 'Record of Processing Activities' in place and knows exactly what personal data is held, where, why and which member of staff has responsibility for managing it.
vi. The Record of Processing Activities lists the lawful basis for processing personal data (including, where relevant, consent). Where special category data is processed, an additional lawful basis is listed.

vii. Has an 'information asset register' in place and knows exactly what personal data is held and where, why and which member of staff has responsibility for managing it.
viii. Information asset register lists the lawful basis for processing personal data (including, where relevant, consent). Where special category data is processed, an additional lawful basis will have also been listed.
ix. Will hold the minimum personal data necessary to enable it to perform its function and will not hold it for longer than necessary for the purposes it was collected for. The school 'retention schedule" supports this.
x. Data held is accurate and up to date and is held only for the purpose it was held for. Systems are in place to identify inaccuracies, such as asking parents to check emergency contact details at suitable intervals.
xi. Provides staff, parents, volunteers, teenagers, and older children with information about how the school looks after their data and what their rights are in a clear Privacy Notice (see section 19).
xii. Has procedures in place to deal with the individual rights of the data subject.
xiii. Carries out Data Protection Impact Assessments (DPIA) where necessary e.g. to ensure protection of personal data when accessed using any remote access solutions or entering into a relationship with a new supplier.
xiv. Has undertaken appropriate due diligence and has data protection compliant contracts in place with any data processors.
xv. Understands how to share data lawfully and safely with other relevant data controllers.
xvi. Has clear and understood policies and routines for the deletion and disposal of data.
xvii. Reports any relevant breaches to the Information Commissioner within 72 hours of becoming aware of the breach as required by law. It also reports relevant breaches to the individuals affected as required by law. In order to do this, it has a policy for reporting, logging, managing, investigating and learning from information risk incidents.
xviii. Has a Freedom of Information Policy which sets out how it will deal with FOI requests.
xix. Provides data protection training for all staff at induction and appropriate refresher training thereafter. Staff undertaking particular data protection functions, such as handling requests under the individual's rights, will receive training appropriate for their function as well as the core training provided to all staff.

19.1 Data on Mobile Devices

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

i. Data will be encrypted, and password protected.
ii. Device will be password protected.
iii. Device will be protected by up-to-date endpoint (anti-virus) software.

iv. Data will be securely deleted from the device, in line with school policy (below) once it has been transferred or its use is complete.

19.1.1 Staff - Personal Data

Staff must ensure that they:

i. At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.
ii. Can recognise a possible breach, understand the need for urgency and know who to report it to within the school.
iii. Can help data subjects understand their rights and know how to handle a request whether verbal or written and know who to pass it to in the school.
iv. Only use encrypted data storage for personal data
v. Will not transfer any school personal data to personal devices.
vi. Use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data.
vii. Transfer data using encryption, a secure email account (where appropriate), and secure password protected devices.

20. 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/carers and is reported to relevant groups:

i. 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.
ii. There are well-established routes to regularly report patterns of online safety incidents and outcomes to school leadership and Governors.
iii. Parents/carers are informed of patterns of online safety incidents as part of the school's online safety awareness raising.
iv. Online safety (and related) policies and procedures are regularly updated in response to the evidence gathered from these reviews/audits/professional debate.
v. 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.

Appendix 1 - Pupil Acceptable Use Agreement for KS3, KS4 and KS5

School Policy

Digital technologies have become integral to the lives of children and young people, both within schools and outside school. These technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. Young people should have an entitlement to safe access to these digital technologies.

This Online Safety Policy Agreement is intended to ensure:

- That young people will be responsible users and stay safe while using the internet and other digital technologies for educational, personal and recreational use.
- That school systems and users are protected from accidental or deliberate misuse that could put the security of the systems and will have good access to digital technologies to enhance their learning and will, in return, expect the pupils to agree to be responsible users.

Online Safety Policy Agreement

I understand that I must use school systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems and other users. This policy applies to all school computers, personal laptops and also any tablets/mobile devices (including phones or smart watches).

I understand that unless directed to by a member of staff, Senior School pupils (Years 7-10) must not use mobile devices during the school day, with the exception that riders are advised to carry a mobile device when they are out hacking or working with horses on fields at some distance from the Equestrian Centre. Senior School pupils (Yr 7-10) who choose to bring a mobile device with them to school should secure it in their locker during the school day. Tablets that can access mobile data are not permitted at Stonar. Pupils in year 11 and Sixth Form are permitted to use their mobile device in the library for work purposes and during break times for personal use in tutor rooms and social spaces. Boarders (excluding sixth formers) are required to hand in their mobile phones (and other portable devices as requested) to the duty member of staff before bedtime; they can be collected before school at morning roll call.

I understand that mobile devices must never be used in changing rooms or toilets, when moving about the school campus, at the front of school, in corridors, or the La Cantina regardless of the time of day / day of the week.

I understand that access to the internet must be via School Wi-Fi. Use of VPN's and 'Hot spotting' is not allowed.

For my own personal safety

- I understand that the schools will monitor my use of the systems, devices and digital communications.
- Personal mobile devices must be clearly named and have passcodes enabled

- I will keep my username and password safe and secure – I will not share it, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may steal it.
- I will be aware of "stranger danger", when I am communicating on-line.
- Identity theft is an online danger that is increasing. I will not disclose or share personal information about myself, my family or others when on-line (this could include names, addresses, email addresses, telephone numbers, age, gender, date of birth, educational details, location, financial details etc.) I will be aware that uploading digital photographs taken from a mobile device might reveal my precise GPS location at a given date and time, and therefore may reveal movements and locations to third parties. It is recommended to avoid using photographs to identify yourself online and use an avatar or cartoon image as a profile picture instead.
- If I arrange to meet people off-line that I have communicated with on-line, I will do so in a public place and take an adult with me.
- I will immediately report any unpleasant, threatening, extremist, inappropriate, suspicious or sexual material or messages or anything that makes me feel uncomfortable when I see it on-line to the Deputy Head Pastoral or Houseparent or teacher (and to the authorities where appropriate).

I understand that everyone has equal rights to use technology as a resource and

- I understand that the school's systems and devices are primarily intended for educational use and that I will not use them for personal or recreational use unless I have permission.
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not use the school's systems or devices for on-line gaming, on-line gambling, internet shopping, file sharing, or video broadcasting (e.g. YouTube), unless I have permission of a member of staff to do so.

I will act as I expect others to act toward me

- I will respect others' work and property and will not access, copy, remove or otherwise alter any other user's files, without the owner's knowledge and permission.
- I will be polite and responsible when I communicate with others, I will not use strong, aggressive, offensive or inappropriate language, to include homophobic and racist language and I appreciate that others may have different opinions.
- I will not take or distribute information/images about a third party/ member of the school community without their permission. I will not publish or share any information that defames, undermines, misrepresents, or tarnishes the reputation of the school or its users.
- Electronic communication between staff and pupils must only be part of approved school activities, and only via approved forms of communication (for example, school email, MS Teams, SMHW, Kerboodle).
- I will not be a cyberbully and will report any unpleasant behaviour.

I recognise that the school has a responsibility to maintain the security and integrity of the technology it offers me and to ensure the smooth running of the school

- I will only use my own personal devices (mobile phones/USB devices etc.) in school if I have permission. I understand that, if I do use my own devices in the school, I will follow the expectations set out in this agreement, in the same way as if I was using school equipment.
- I understand the risks and will not try to upload, download, access, create or send any materials which are illegal, offensive or inappropriate or may cause harm or distress to others, nor will I try to use any programmes or software that might allow me to bypass the filtering/security systems in place to prevent access to such materials.
- I will immediately report any damage or faults involving equipment or software; however, this may have happened.
- I will not open any hyperlinks in emails or any attachments to emails, unless I know and trust the person/organisation who sent the email, or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes)
- I will not install or attempt to install or store programmes of any type on any school device, nor will I try to alter computer settings.
- I will only use social media sites with permission and at the times that are allowed.

When using the internet for research or recreation, I recognise that:

- I should ensure that I have permission to use the original work of others in my own work.
- Where work is protected by copyright, I will not try to download copies (including music and videos)
- When I am using the internet to find information, I should take care to check that the information that I access is accurate, as I understand that the work of others may not be truthful and may be a deliberate attempt to mislead me.
- I understand any individual found using a mobile device to cheat in examinations or other formal testing opportunities will face disciplinary action.

I understand that I am responsible for my actions, both in and out of school:

- I understand that the school also has the right to take action against me if I am involved in incidents of inappropriate behaviour, that are covered in this agreement, when I am out of school and where they involve my membership of the school community (examples would be online-bullying, use of images or personal information).
- I understand that if I fail to comply with this AUA, I may be subject to disciplinary action. This could include loss of access to the school network/internet, detentions, suspensions, contact with parents and in the event of illegal activities involvement of the police.

Liability

I understand that Stonar accepts no responsibility for the repair or replacement of mobile devices that are lost, stolen or damaged whilst on school property or during extra-curricular activities, trips or when travelling to and from School on School transport. It is recommended that pupils/parents take out their own insurance for all such devices.

I understand that the School makes no guarantee, whether expressed or implied, for the information carried over the network or internet service it provides. Although the systems offer a very high level of protection, the School cannot be held responsible or accept liability for any damage or loss of data, or the consequences of such damage or loss, whilst any member of the School is on the school

system. The School accepts no liability for any damage caused by any type of computer virus; however, it originates. The School accepts no liability in the unlikely event that damage is sustained to a privately owned computer as a result of its being connected to the network.

Please complete the sections on the next page to show that you have read, understood and agree to the expectations included in the AUA. If you do not sign and return this agreement, access will not be granted to school systems and devices.

Pupil Online Safety Policy Agreement Form

Please complete the sections below to show that you have read, understood and agree to the expectation included in the AUA. If you do not sign and return this agreement, access will not be granted to school systems.

I have read and understand the above and agree to follow these guidelines when:

- I use the school's systems and devices (both in and out of school)
- I use my own devices in the school (when allowed) e.g. mobile phones, gaming devices USB devices, cameras etc.
- I use my own equipment out of the school in a way that is related to me being a member of this school e.g. communicating with other members of the school, accessing school email, VLE, website etc.

Name of Pupil: .....

Group/Class: .....

Signed: .....

Date: .....

Appendix 2 - Online Safety Policy Agreement for KS2

Introduction

Digital technologies have become integral to the lives of children and young people, both within and outside schools. These technologies are powerful tools, which open-up new opportunities for everyone. They can stimulate discussion, encourage creativity, and stimulate awareness of context to promote effective learning. Learners should have an entitlement to safe access to these digital technologies.

This online safety policy agreement is intended:

i. To ensure that learners will have good access to devices and online content, be responsible users and stay safe while using digital technologies for educational, personal and recreational use.
ii. To help learners understand good online behaviours that they can use in school, but also outside school.
iii. To protect school devices and networks from accidental or deliberate misuse that could put the security of the systems and users at risk.

Online Safety Policy Agreement

Prep School pupils are not permitted to have a personal mobile device during the school day without the express permission of the Head of Prep School. In the circumstance children are allowed to bring the phone/device to school, these must be handed to the class teacher and securely stored until handed back just before the child goes home.

Boarders are required to hand in their mobile phones (and other portable devices, as requested) to the duty member of staff before bedtime; they can be collected after school the following day.

For my own Personal Safety

When I use devices, I must behave responsibly to help keep myself and other users safe online and to look after the devices. This policy applies to all school computers, personal laptops and also any tablets/mobile devices (including phones or smart watches).

- I understand that what I do online will be supervised and monitored and that I may not be allowed to use devices in school unless I follow these expectations and use them responsibly.
- I will only visit internet sites that adults have told me are safe to visit.
- I will keep my username and password safe and secure and not share it with anyone else.
- I will be aware of "stranger danger" when I am online.
- I will not share personal information about myself or others when online.

- I will immediately tell an adult (teacher) if I see anything that makes me feel uncomfortable when I see it online.

For the Safety of the Devices I Use

- I will handle all the devices carefully and only use them if I have permission.
- I will not try to alter the settings on any devices or try to install any software or programmes.
- I will tell an adult if a device is damaged or if anything else goes wrong.
- I will only use the devices to do things that I am allowed to do.

I will Think About How my Behaviour Online Might Affect Other People

- When online, I will act as I expect others to act toward me.
- I will not copy anyone else's work or files without their permission.
- I will be polite and responsible when I communicate with others and will not use aggressive, offensive or inappropriate language.
- I will not take or distribute information or images of other people without their permission. I will not publish or share any information that is unkind about the School or the people in it.
- I will not be a cyberbully and will report any unpleasant behaviour.
- Electronic communication between staff and pupils must only be part of approved school activities, and only via approved forms of communication (for example, school email, MS Teams, SMHW, Kerboodle).

I Know that there are Other Rules that I Need to Follow:

- I am not allowed my own devices in School without permission from the Head and my parents.
- When I am using the internet to find information, I should take care to check that the information is accurate, as I understand that the work of others may not be truthful and may be a deliberate attempt to mislead me.

I Understand that I am Responsible for My Actions, Both In and Out of School

- I know that I am expected to follow these expectations in School and that I should behave in the same way when out of School as well.
- I understand that if I do not follow these expectations, there will be consequences which could include not being able to use school devices and parents being contacted.

Liability

Stonar accepts no responsibility for the repair or replacement of mobile devices that are lost, stolen or damaged whilst on School property or during extra-curricular activities, trips

or when travelling to and from School on School transport. It is recommended that pupils/parents take out their own insurance for all such devices.
The School makes no guarantee, whether expressed or implied, for the information carried over the network or internet service it provides. Although the systems offer a very high level of protection, the School cannot be held responsible, or accept liability, for any damage or loss of data, or the consequences of such damage or loss, whilst any member of the School is on the school system. The School accepts no liability for any damage caused by any type of computer virus; however, it originates. The School accepts no liability in the unlikely event that damage is sustained to a privately-owned computer as a result of its being connected to the network.

Pupil Online Safety Policy Agreement Form for Key Stage 2

By signing the class agreement sheet, below, you are showing that you have read, understood, and agree to the expectations included in the Online Safety Policy Agreement for KS2, above.

If you do not sign and return this agreement, access will not be granted to school systems.
I have read and understand the above and agree to follow these guidelines when:

I use the school systems and devices.
I use my own equipment out of the school in a way that is related to me being a member of this school eg communicating with other members of the school, using school email or MS Teams etc.

Class:_____ Date:_____

Name	Signed		Name	Signed

Appendix 3 - Pupil Online Safety Policy Agreement for Younger Learners (Foundation/KS1)

In line with EYFS regulations, personal mobile devices are not allowed in the EYFS setting.

This is how we stay safe when we use computers:

Years 1 and 2: Children will sign a child-friendly copy of the AUA.
In Early Years: Staff will display a poster and discuss this appropriately with the children.

The poster will contain the following statements:

- I will ask a teacher or suitable adult if I want to use the computers/tablets.
- I will only use activities that a teacher or suitable adult has told or allowed me to use.
- I will take care of computers/tablets and other equipment.
- I will ask for help from a teacher or suitable adult if I am not sure what to do or if I think I have done something wrong.
- I will tell a teacher or suitable adult if I see something that upsets me on the screen.
- I know that if I break the expectations, I might not be allowed to use a computer/tablet.

I want to feel safe all the time and I agree that I will:

- always keep my passwords a secret
- only open pages which my teacher has said are OK
- only work with people I know in real life
- tell my teacher if anything makes me feel scared or uncomfortable on the internet
- make sure all messages I send are polite
- show my teacher if I get a nasty message
- not reply to any nasty message or anything which makes me feel uncomfortable
- not give my phone number to anyone who is not a friend in real life
- only email people I know or if my teacher agrees
- only use my school email
- not use social media at school unless working with a teacher
- talk to my teacher before using anything on the internet
- not tell people about myself online (I will not tell them my name, anything about my home and family and pets)
- not upload photographs of myself without asking a teacher
- never agree to meet a stranger

Appendix 4 - Prep Parent/Carer Online Safety Policy Agreement

Digital technologies have become integral to the lives of children and young people, both within schools and outside school. These technologies provide powerful tools, which open new opportunities for everyone. They can stimulate discussion, promote creativity, and stimulate awareness of context to promote effective learning. Young people should have an entitlement to safe internet access at all times.

This online safety policy is intended to ensure:

- That young people will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- That school systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- That parents and carers are aware of the importance of online safety and are involved in the education and guidance of young people with regard to their on-line behaviour.

The school will try to ensure that pupils have good access to digital technologies to enhance their learning and will, in return, expect the pupils to agree to be responsible users. I understand that the school has discussed the Acceptable Use Agreement (AUA) with my son/daughter and that they have received, or will receive, online safety education to help them understand the importance of safe use of technology and the internet – both in and out of school. A copy of the pupil AUA is attached to this permission form, so that parents/carers will be aware of the school expectations of the young people in their care.

I understand that the school will take every reasonable precaution, including monitoring and filtering systems, to ensure that young people will be safe when they use the internet and systems. I also understand that the school cannot ultimately be held responsible for the nature and content of materials accessed on the internet and using mobile technologies.

I understand that my son's/daughter's activity on the systems will be monitored and that the school will contact me if they have concerns about any possible breaches of the AUA.

I will encourage my child to adopt safe use of the internet and digital technologies at home and will inform the school if I have concerns over my child's online safety.

As the parent/carer of the above pupil, I give permission for my son/daughter to have access to the digital technologies at school. Parents are requested to sign the permission form below to show their support of the school in this important aspect of the school's work.

Permission Form

Parent/Carers Name: .....

Pupil Name: .....

Online Safety Policy Agreement for Pupils
The online safety policy agreement signed by pupils is sent as a separate attachment.

PARENTAL CONSENT FORM (Use of Images)

Stonar makes various uses of images of pupils during their time at school.

Some of these are essential for administration and the safety of pupils, such as CCTV and for your child's online ID. Photos of your child, including photos of pupils at work or playing games may be used in and around the School and may be included on the School website/social media platforms or as part of a School prospectus, magazine / newspaper article or other marketing materials where they may be seen by people outside of the school.

To comply with the General Data Protection Regulations (GDPR) and the Data Protection Act 2018, we need your permission before we can photograph or make any recordings of your child.

Please indicate below if you **consent for the time being** to your child's image being used for the purposes of promoting the school, including images where your child is a particular focus of a shot. Where appropriate, owing to the pupil's age or nature of the use, we will seek verbal or written consent before publishing any image where that pupil is identified by name, but not usually when included as part of a larger group or team shot.

NAME OF CHILD:
DATE OF BIRTH:

Tick ☐ Yes, I consent to my child's image being used in the manner described.
You may withdraw consent at any time in the future, subject to the notice below. If you object to such uses until further notice, please indicate below. In ensuring we can give effect to your wishes, it will also assist us if you are able to give reasons.

Tick ☐ No, I object to all non-essential uses of my child's image without specific consent.
Please give reasons for withholding consent [optional]:

Please be aware that objecting as above i not necessarily mean that the School will not continue to process images of your child that are either necessary for administration for the School, or separately consented by you or your child (eg uses for biometrics), or the school magazine or prospectus or third party publications (for example, where we have placed an advert or provided an image to a newspaper).

An adult with parental responsibility should sign this Consent Form together with the pupil, if aged over 13. The School is entitled to treat any instruction, authority, request or prohibition received from any person who has signed with Consent Form as having been given on behalf of both or all such persons, including others with parental responsibility.

Signed by adult with parental responsibility: _____

Print name: _____

Relationship to child: _____

Signed by pupil, if aged over 13: _____

Print name: _____

Date:

If you have any questions about this form, please contact the Admissions Department.

Appendix 5 - Staff (and Volunteer) Online Safety Policy Agreement

School Policy

New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school. The internet and other digital information and communications technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. They also bring opportunities for staff to be more creative and productive in their work. All users should have an entitlement to safe access to the internet and digital technologies at all times.

This online safety policy is intended to ensure:

- That staff and volunteers will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- That school systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- That staff are protected from potential risk in their use of technology in their everyday work.

The school will try to ensure that staff and volunteers will have good access to digital technology to enhance their work, to enhance learning opportunities for learning and will, in return, expect staff and volunteers to agree to be responsible users.

Online Safety Policy Agreement

I understand that I must use school systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems and other users. I recognise the value of the use of digital technology for enhancing learning and will ensure that pupils receive opportunities to gain from the use of digital technology. I will, where possible, educate the young people in my care in the safe use of digital technology and embed online safety in my work with young people.
I understand this policy applies to all school computers, personal laptops and also any tablets / mobile devices (including phones or 'smart watches') used in school.
In line with EYFS regulations, personal mobile devices are not allowed in the EYFS setting of the school site.

Staff * mobile devices should at all times be set to silent / vibrate and may not be used in changing rooms, in the dining hall, when moving around the school campus unless an emergency phone or in an emergency situation.*Exceptions to this are made for members of the equestrian, IT Support, Marketing and maintenance departments who use mobile phones as part of their role in school; furthermore, equestrian staff are advised to carry a mobile device when they are out hacking or working with horses on fields at some distance from the Equestrian Centre.

For my professional and personal safety:

- I understand that the school will monitor my use of the school digital technology and communications systems.

- I understand that the rules set out in this agreement also apply to use of these technologies (e.g. laptops, email, VLE etc.) out of school, and to the transfer of personal data (digital or paper based) out of school.
- I understand that the school digital technology systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within the policies and expectations set down by the school.
- Staff 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. Those images should only be taken on school devices. Personal devices must not be used to take photographs/videos of pupils for any reason.
- I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may steal it.
- Identity theft is an online danger that is increasing. Staff are recommended not to upload or reveal personal details of themselves, their family or other Stonar users online (e.g. address, phone number, date of birth, financial details, passwords, etc.) Images and/or comments that could embarrass school users and families should not be uploaded. School members would be aware that uploading digital photographs taken from a mobile device might reveal their precise GPS location at a given date and time, and therefore may reveal movements and locations to third parties. It is recommended to avoid using photographs to identify yourself online and use an avatar or cartoon image as a profile picture instead.
- I will immediately report any illegal, inappropriate or harmful material or incident or suspicious online sexual advances or threatening behaviour, I become aware of, to a member of the Leadership Team and safeguarding concerns to the Designated Safeguarding Lead or in their absence a member of the safeguarding team.

I will be professional in my communications and actions when using school systems:

- I will not access, copy, remove or otherwise alter any other user's files, without their express permission.
- I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will ensure that when I take and/or publish images of others I will do so with their permission and in accordance with the school's policy on the use of digital/video images. I will not use my personal equipment to record these images. Where these images are published (e.g. on the school website/VLE) it will not be possible to identify by name, or other personal information, those who are featured.
- It is forbidden to publish or share any information that defames, undermines, misrepresents, or tarnishes the reputation of the school or its users.
- I will only use social networking sites in school in accordance with the school's policies.
- I will only communicate with pupils and parents/carers using official school systems (for example, school email, MS Teams, SMHW, Kerboodle). Any such communication will be professional in tone and manner.
- I will not engage in any on-line activity that may compromise my professional responsibilities.

The school has the responsibility to provide safe and secure access to technologies and ensure the smooth running of the school:

- When I use my mobile devices in school, I will follow the expectations set out in this agreement, in the same way as if I was using school equipment. I will also follow any additional expectations set by the school about such use. I will ensure that any such devices are protected by up-to-date anti-virus software and are free from viruses.
- I will not use personal email addresses on the school's ICT systems.
- I will not open any hyperlinks in emails or any attachments to emails, unless the source is known and trusted, or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes)
- I will ensure that my data is regularly backed up, in accordance with relevant school policies.
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, terrorist or extremist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering/security systems in place to prevent access to such materials.
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings, unless this is allowed in school policies.
- I will not disable or cause any damage to school equipment, or the equipment belonging to others.
- I will only transport, hold, disclose or share personal information about myself or others, as outlined in the School Personal Data Policy (or other relevant policy). Where digital personal data is transferred outside the secure local network, it must be encrypted. Paper based documents containing personal data must be held in lockable storage.
- I understand that data protection policy requires that any staff or pupil data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by school policy to disclose such information to an appropriate authority.
- I will immediately report any damage or faults involving equipment or software; however this may have happened.

When using the online systems in my professional capacity or for school sanctioned personal use:

- I will ensure that I have permission to use the original work of others in my own work.
- Where work is protected by copyright, I will not download or distribute copies (including music and videos).

I understand that I am responsible for my actions in and out of the school:

- I understand that this acceptable use policy applies not only to my work and use of school's digital technology equipment in school, but also applies to my use of school systems and equipment off the premises and my use of personal equipment on the premises or in situations related to my employment by the school.
- I understand that if I fail to comply with this acceptable use agreement, I could be subject to disciplinary action. This could include a warning, a suspension, referral to Board of Proprietors Directors and/or the Local Authority and in the event of illegal activities the involvement of the police.

Liability

- Stonar accepts no responsibility for the repair or replacement of mobile devices that are lost, stolen or damaged whilst on school property or during extra-curricular activities, trips or when travelling to and from School on School transport. It is recommended that staff take out their own insurance for all such devices.
- The School makes no guarantee, whether expressed or implied, for the information carried over the network or internet service it provides. Although the systems offer a very high level of protection, the School cannot be held responsible or accept liability for any damage or loss of data, or the consequences of such damage or loss, whilst any member of the School is on the school system. The School accepts no liability for any damage caused by any type of computer virus; however, it originates. The School accepts no liability in the unlikely event that damage is sustained to a privately owned computer as a result of its being connected to the network.

I have read and understand the above and agree to use the school digital technology systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) within these guidelines.

Staff/Volunteer Name: .....

Signed: .....

Date: .....

Appendix 6 - Online Safety Policy Agreement for Community Users/Visitors/Hirers

This online safety policy agreement is intended to ensure:

- That community users of school digital technologies will be responsible users and stay safe while using these systems and devices.
- That school systems, devices and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- That users are protected from potential harm in their use of these systems and devices.

Online Safety Policy Agreement

I understand that I must use school systems and devices in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems, devices and other users. This agreement will also apply to any personal devices that I bring into the school:

- I understand that my use of school systems and devices will be monitored.
- I will not use a personal device that I have brought into school for any activity that would be inappropriate in a school setting.
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, terrorist and extremist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering/security systems in place to prevent access to such materials.
- I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person.
- I will not access, copy, remove or otherwise alter any other user's files, without permission.
- I will ensure that if I take and/or publish images of others I will only do so with their permission. I will not use my personal equipment to record these images, without permission. If images are published it will not be possible to identify by name, or other personal information, those who are featured.
- I will not publish or share any information I have obtained whilst in the school on any personal website, social networking site or through any other means, unless I have permission from the school.
- I will not, without permission, make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not install or attempt to install programmes of any type on a school device, nor will I try to alter computer settings, unless I have permission to do so.
- I will not disable or cause any damage to school equipment, or the equipment belonging to others.
- I will immediately report any damage or faults involving equipment or software, whatever the cause.
- I will ensure that I have permission to use the original work of others in my own work.
- Where work is protected by copyright, I will not download or distribute copies (including music and videos).
- I understand that if I fail to comply with this acceptable use agreement, the school has the right to remove my access to school systems/devices.

As the Hirer, you understand that the school systems (including Wi-fi) are for you and your team only and will take responsibility for all the rules within if access is given to your customers and these rules are not abided by.

I have read and understand the above and agree to use the school systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) within these guidelines.

Name: Signed: Date:

Appendix 7 - School Policy: Online Safety Group Terms of Reference

1. Purpose

To provide a consultative group that has wide representation from the school, with responsibility for issues regarding online safety and the monitoring the online safety policy including the impact of initiatives.

2. Membership

2.1. The Online Safety Group will seek to include representation from all stakeholders.

The composition of the group should include.

- EMG & SLT member/s
- DSL/OSL & DDSL
- Teaching staff member
- Support staff member
- Proprietor representative responsible for Online Safety at Stonar
- Parent/Carer
- IT Support Provider
- Community users (where appropriate)
- Pupil representation – for advice and feedback.

2.2. Other people may be invited to attend the meetings at the request of the Chairperson on behalf of the committee to provide advice and assistance where necessary.

2.3. Committee members must declare a conflict of interest if any incidents being discussed directly involve themselves or members of their families.

2.4. Committee members must be aware that many issues discussed by this group could be of a sensitive or confidential nature.

2.5. When individual members feel uncomfortable about what is being discussed they should be allowed to leave the meeting with steps being made by the other members to allow for these sensitivities

3. Chairperson (DSL)

The Committee should select a suitable Chairperson from within the group. Their responsibilities include:

- Scheduling meetings and notifying members.
- Inviting other people to attend meetings when required.
- Guiding the meeting according to the agenda and time available.
- Ensuring all discussion items end with a decision, action or definite outcome.
- Making sure that notes are taken at the meetings and that these with any action points are distributed as necessary.

4. Meetings

Meetings shall be held termly.

5. Functions

These are to assist the DSL/OSL with the following:

- To keep up to date with new developments in the area of online safety
- To (at least) annually review and develop the online safety policy in line with new technologies and incidents.
- To monitor the delivery and impact of the online safety policy
- To monitor the log of reported online safety incidents (anonymous) to inform future areas of teaching/learning/training.
- To co-ordinate consultation with the whole school community to ensure stakeholders are up to date with information, training and/or developments in the area of online safety. This could be carried out through the following list which does not tend to be an exhaustive list:
  -Staff meetings
  -Learner forums (for advice and feedback)
  -Governors' meetings
  -Surveys/questionnaires for pupils, parents/carers and staff
  -Parents evenings
  -Website/newsletters
  -Online safety events
  -Internet Safety Day (annually held on the second Tuesday in February)
- To ensure that monitoring is carried out of Internet sites used across the schools.
- To monitor filtering/change control logs (e.g. requests for blocking/unblocking sites).
- To monitor the safe use of data across the schools
- To monitor incidents involving cyberbullying for staff and learners

6. Amendments

The terms of reference shall be reviewed annually from the date of approval. They may be altered to meet the current needs of all committee members, by agreement of the majority. The above Terms of Reference for Stonar School have been agreed.

Signed by (EMG): ..... Date: .....

Date for review: .....

Appendix 8 - Online Safety Incident Log Form

This is recorded electronically.

Online Safety Incident Log Form						
Date	Time	Incident	Action Taken		Incident Reported By	Signature
			What?	By Whom?		

Appendix 9 - Legislation Information

The following is a summary of legislative framework that underpins this online safety policy.

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 "Cybercrime – 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 Headteachers, to such extent as is reasonable, to regulate the behaviour of learners 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 Headteachers (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/carer 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

Appendix 10 - Links to other Organisations or Documents

The National Crime Agency

The NCA website 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. The following links provide additional advice or guidance with regard to online safety:

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 carers

SWGfL – Online Safety Guidance for Parents & Carers
Vodafone Digital Parents Magazine
Childnet Webpages for Parents & Carers

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

Glossary of Terms

AUP/AUA	Acceptable Use Policy/Agreement
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
MASH	Multi Academy Safeguarding Hub
MIS	Management Information System
OSP/OSA	Online Safety Policy/Agreement.
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