Maidstone Grammar School
for Girls

Non sibi sed omnibus

Online Safety Policy

Governor Policy

2025-2026

History Log

Last Revised	Revised By	Ratified By Governors	Next Review Date	Time Scale
April 2024	Deborah Stanley	23.05 2024	April 2025	Annually
April 2025	Ben White	30.04.2025	April 2026	Annually

Contact: Mr B White, Assistant Headteacher

A forward-thinking community with a tradition of excellence

Table of Contents

Scope of the Online Safety Policy

This Online Safety Policy outlines the commitment of Maidstone Grammar School for Girls (MGGS) to safeguard members of our school community online in accordance with statutory guidance and best practice. This Online Safety Policy applies to all members of the school community (including staff, students, 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).

MGGS 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.

Schedule for Development, Monitoring and Review

This Online Safety Policy was approved by the school's governing body on 30th April 2025. This 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. This implementation of this policy will be monitored by the Leadership Team together with the Governors Resources committee who will receive a report on its implementation at least once a year.

Should any serious online safety incidents take place the school will inform the local authority safeguarding team, police etc, as appropriate.

Policy and Leadership

Responsibilities

To ensure the online safeguarding at MGGS 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. The following outlines the online safety roles and responsibilities of individuals and groups within the school.

Headteacher and Senior Leaders

- The headteacher has a duty of care for ensuring the safety (including online safety) of members of MGGS and fostering a culture of safeguarding, though the day-to-day responsibility for online safety may be delegated to the Online Safety Lead.
- The headteacher and members of the senior leadership team should be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff.
- The headteacher/senior leaders are responsible for ensuring that the Online Safety Lead, 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.
- The headteacher/senior leaders will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal online safety monitoring role.

- The headteacher/senior leaders will receive regular monitoring reports from the Online Safety Lead.

Governors

Governors are responsible for the approval of the Online Safety Policy and for reviewing the effectiveness of the policy.

This review will be carried out by the Curriculum Committee. A member of the governing body will take on the role of Online Safety Governor to include:

- regular meetings with the Online Safety Lead
- regularly receiving (collated and anonymised) reports of online safety incidents
- checking that provision outlined in the Online Safety Policy (e.g. online safety education provision and staff training is taking place as intended)
- reporting to relevant governors group/meeting
- occasional review of the filtering change control logs and the monitoring of filtering logs (where possible)

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

Online Safety Lead

The Online Safety Lead will:

- work closely on a day-to-day basis with the Designated Safeguarding Lead (DSL)
- take day-to-day responsibility for online safety issues, being aware of the potential for serious child protection concerns
- have a leading role in establishing and reviewing the school online safety policies/documents
- promote an awareness of and commitment to online safety education / awareness raising across the school and beyond
- liaise with curriculum leaders to ensure that the online safety curriculum is planned, mapped, embedded and evaluated
- ensure that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place and the need to immediately report those incidents
- receive reports of online safety incidents and create a log of incidents to inform future online safety developments
- provide (or identify sources of) training and advice for staff/governors/parents/carers/learners
- liaise with technical staff, pastoral staff and support staff (as relevant)
- meet regularly with the online safety governor to discuss current issues, review (anonymised) incidents and if possible, filtering and monitoring logs

Designated Safeguarding Lead (DSL)

The DSL should be trained in online safety issues and be aware of the potential for serious safeguarding issues to arise from:

- sharing of personal data
- access to illegal/inappropriate materials
- inappropriate online contact with adults/strangers
- potential or actual incidents of grooming
- online bullying

Curriculum Leads

Curriculum Leads will work with the Online Safety Lead to develop a planned and coordinated online safety education programme.

Teaching and Support Staff

School staff are responsible for ensuring that:

- they have an awareness of current online safety matters/trends and of the current school Online Safety Policy and practices
- they understand that online safety is a core part of safeguarding
- they have read, understood the staff acceptable use agreement (AUA)
- they immediately report any suspected misuse or problem to the DSL for investigation/action, in line with the school safeguarding procedures
- online safety issues are embedded in all aspects of the curriculum and other activities
- ensure learners understand and follow the Online Safety Policy and acceptable use agreements
- 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 - including supporting the consistent use of lockable phone pouches to support online safety school years 7-11
- in lessons where internet use is pre-planned learners should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches
- where lessons take place using live-streaming or video-conferencing, staff must have full regard to national safeguarding guidance and local safeguarding policies and should take note of the guidance contained in the SWGfL Safe Remote Learning Resource
- have a zero-tolerance approach to incidents of online-bullying, sexual harassment, discrimination, hatred etc
- they model safe, responsible, and professional online behaviours in their own use of technology, including out of school and in their use of social media.

Systems Manager/Technical Staff

The Systems manager/technical staff is responsible for ensuring that:

- 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
- the school technical infrastructure is secure and is not open to misuse or malicious attack
- the school meets (as a minimum) the required online safety technical requirements as identified by the local authority or other relevant body
- there is clear, safe, and managed control of user access to networks and devices
- 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
- the use of technology is regularly and effectively monitored in order that any misuse/attempted misuse can be reported to the headteacher for investigation and action
- the filtering policy is applied and updated on a regular basis and its implementation is not the sole responsibility of any single person
- monitoring software/systems are implemented and regularly updated as agreed in school policies

Students

- are responsible for using the school digital technology systems in accordance with the student acceptable use agreement and Online Safety Policy
- should understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- should know what to do if they or someone they know feels vulnerable when using online technology
- should understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the school's Online Safety Policy covers their actions out of school, if related to their membership of the school

Parents and Carers

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

- publishing the school Online Safety Policy on the school website
- providing them with a copy of the learners' acceptable use agreement via the student shared drive
- publish information about appropriate use of social media relating to posts concerning the school
- seeking their permissions concerning digital images, cloud services etc
- parents'/carers' evenings, newsletters, website, social media and information about national/local online safety campaigns and literature

Parents and carers will be encouraged to support the school in:

- reinforcing the online safety messages provided to learners in school
- the use of their children's personal devices in the school - including supporting the use of lockable phone pouches for students in KS3 and KS4

Policy

Acceptable use

The school has defined what it regards as acceptable/unacceptable use and this is shown in the tables below. The Online Safety Policy and acceptable use agreements define acceptable use at the school.

The acceptable use agreements will be communicated/re-enforced through:

- the curriculum
- staff induction
- digital signage
- posters/notices around where technology is used
- communication with parents/carers
- built into education sessions
- school website
- 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:**					**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 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**		
	Any other information which may be offensive to others or breaches the integrity of the ethos of the school or brings the school into disrepute				**X**	

Consideration should be given for the following activities when undertaken for non-educational purposes:	Staff and other adults				Learners			
	Not allowed	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission/ awareness
Online gaming								
Online shopping/commerce								
File sharing								
Social media								
Messaging/chat								
Entertainment streaming e.g. Netflix, Disney+								
Use of video broadcasting, e.g. YouTube, Twitch, TikTok								
Mobile phones may be brought to school								
Use of mobile phones for learning at school								
Use of mobile phones in social time at school								
Taking photos on personal mobile phones/cameras								
Use of other personal devices, e.g. tablets, gaming devices								
Use of personal e-mail in school, or on school network/wi-fi								
Use of school e-mail for personal e-mails								

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

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

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 which will need intervention.

The school will ensure:

- there are clear reporting routes which are understood and followed by all members of the school community which are consistent with the school safeguarding procedures, and with the whistleblowing, complaints and managing allegations policies
- all members of the school community will be made aware of the need to report online safety issues/incidents
- reports will be dealt with as soon as is practically possible once they are received
- the designated safeguarding lead, online safety lead and other responsible staff have appropriate skills and training to deal with online safety risks
- if there is any suspicion that the incident involves any illegal activity or the potential for serious harm the incident must be escalated through the agreed school safeguarding procedures
- any concern about staff misuse will be reported to the headteacher, unless the concern involves the headteacher, in which case the complaint is referred to the chair of governors
- where there is no suspected illegal activity, devices may be checked using the following procedures:
    - one or more senior members of staff, including heads of study, should be involved in this process. This is vital to protect individuals if accusations are subsequently reported
    - conduct the procedure using a designated device that will not be used by 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.
    - ensure that the relevant staff have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection)
    - record the URL of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed, and attached to the form.

    - once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does, then appropriate action will be required and could include the following:
        - internal response or discipline procedures
        - police involvement and/or action
- it is important that those reporting an online safety incident have confidence that the report will be treated seriously and dealt with effectively
- there are support strategies in place e.g., peer support for those reporting or affected by an online safety incident
- incidents should be logged on Myconcern
- relevant staff are aware of external sources of support and guidance in dealing with online safety issues, e.g. local authority; police; Professionals Online Safety Helpline; Reporting Harmful Content; CEOP.
- those involved in the incident will be provided with feedback about the outcome of the investigation and follow up actions
- learning from the incident (or pattern of incidents) will be provided (as relevant and anonymously) to:
    - staff, through regular briefings
    - students, through assemblies/lessons
    - parents/carers, through newsletters, school social media, website
    - governors, through regular safeguarding updates
    - 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.

An Online safety incident flowchart is given in the Appendices.

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. It is intended that incidents of misuse will be dealt with through normal behaviour/disciplinary procedures.

Examples of potential breaches could include:

- Deliberately accessing or trying to access material that could be considered illegal
- Attempting to access or accessing the school network, using another user's account (staff or learner) or allowing others to access school network by sharing username and passwords
- Corrupting or destroying the data of other users
- Sending an e-mail, text or message that is regarded as offensive, harassment or of a bullying nature
- Unauthorised downloading or uploading of files or use of file sharing
- Using proxy sites or other means to subvert the school's filtering system
- Accidentally accessing offensive or pornographic material and failing to report the incident.
- Deliberately accessing or trying to access offensive or pornographic material
- Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act
- Unauthorised use of digital devices (including taking images)
- Unauthorised use of online services

- Actions which could bring the school into disrepute or breach the integrity or the ethos of the school
- Continued infringements of the above, following previous warnings or sanctions

Responding to Staff Actions

Potential staff breaches could include:

- deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities)
- deliberate actions to breach data protection or network security rules
- deliberately accessing or trying to access offensive or pornographic material
- corrupting or destroying the data of other users or causing deliberate damage to hardware or software
- using proxy sites or other means to subvert the school's filtering system.
- unauthorised downloading or uploading of files or file sharing
- breaching copyright or licensing regulations
- allowing others to access school networks by sharing username and passwords or attempting to access or accessing the school network, using another person's account
- sending an e-mail, text or message that is regarded as offensive, harassment or of a bullying nature
- using personal e-mail/social networking/messaging to carry out digital communications with learners and parents/carers
- inappropriate personal use of the digital technologies e.g. social media / personal e-mail
- careless use of personal data, e.g. displaying, holding or transferring data in an insecure manner
- actions which could compromise the staff member's professional standing
- actions which could bring the school into disrepute or breach the integrity or the ethos of the school
- failing to report incidents whether caused by deliberate or accidental actions
- continued infringements of the above, following previous warnings or sanctions

Staff/Volunteers

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

- a planned programme of formal online safety and data protection training will be made available to all staff. This will be regularly updated and reinforced. An audit of the online safety training needs of all staff will be carried out regularly
- the training will be an integral part of the school's annual safeguarding and data protection training for all staff
- all new staff will receive online safety training as part of their induction programme, ensuring that they fully understand the school online safety policy and acceptable use agreements. It includes explicit reference to classroom management, professional conduct, online reputation and the need to model positive online behaviours
- the online safety lead and designated safeguarding lead (or other nominated person) will receive regular updates through attendance at external training events, (e.g. UKSIC / SWGfL / MAT / LA / other relevant organisations) and by reviewing guidance documents released by relevant organisations

- this Online Safety Policy and its updates will be presented to and discussed by staff in staff/team meetings/INSET days
- the online safety lead (or other nominated person) will provide advice/guidance/training to individuals as required.

Governors

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

- attendance at training provided by the local authority or other relevant organisation (e.g., SWGfL)
- participation in school training / information sessions for staff or parents

A higher level of training will be made available to (at least) the online safety governor.

Families

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

- regular communication, awareness-raising and engagement on online safety issues, curriculum activities and reporting routes
- regular opportunities for engagement with parents/carers on online safety issues through parent/carer evenings etc
- letters, newsletters, website,
- high profile events / campaigns e.g. Safer Internet Day
- reference to the relevant websites/publications, e.g. SWGfL; www.saferinternet.org.uk/; www.childnet.com/parents-and-carers (see Appendix for further links/resources).
- Sharing good practice with other schools in clusters and or the local authority

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.

Filtering

- the school filtering policies are agreed by senior leaders and technical staff and are regularly reviewed and updated in response to changes in technology and patterns of online safety incidents/behaviours
- the school manages access to content across its systems for all users. The filtering provided meets the standards defined in the UK Safer Internet Centre
- access to online content and services is managed for all users
- illegal content (e.g., child sexual abuse images) is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list and the police assessed list of unlawful terrorist content, produced on behalf of the Home Office. Content lists are regularly updated
- there are established and effective routes for users to report inappropriate content

- there is a clear process in place to deal with requests for filtering changes
- 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.)
- DNA/Senso logs are regularly reviewed and alert the school to breaches of the filtering policy, which are then acted upon.
- where personal mobile devices have internet access through the school network, content is managed in ways that are consistent with school policy and practice.

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

Monitoring

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

- the school monitors the use of all school owned devices
- an appropriate monitoring strategy for all users has been agreed and users are aware that all school owned devices are monitored. There is a staff lead responsible for managing the monitoring strategy and processes
- there are effective protocols in place to report abuse/misuse. There is a clear process for prioritising response to alerts that require rapid safeguarding intervention. Management of serious safeguarding alerts is consistent with safeguarding policy and practice
- technical monitoring systems are up to date and managed and logs/alerts are regularly reviewed and acted upon

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

- physical monitoring (adult supervision in the classroom)
- internet use is logged, regularly monitored and reviewed
- DNA/Senso are regularly analysed and breaches are reported to senior leaders
- pro-active alerts inform the school of breaches to the filtering policy, allowing effective intervention
- where possible, school technical staff regularly monitor and record the activity of users on the school technical systems

Technical Security

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

- there will be regular reviews and audits of the safety and security of school technical systems
- servers, wireless systems and cabling are securely located and physical access restricted
- there are rigorous and verified back-up routines, including the keeping of network-separated (air-gapped) copies off-site or in the cloud
- 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 Systems Manager and will be reviewed, at least annually
- all users (adults and learners) 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.

Users must immediately report any suspicion or evidence that there has been a breach of security

- all school networks and systems will be protected by secure passwords. Passwords must not be shared with anyone. All users will be provided with a username and password by the Systems Manager of the Senior Systems Technician who will keep an up-to-date record of users and their usernames. all staff and governors are required to use 2 Factor authentication
- the master account passwords for the school systems are kept in a secure place, e.g. school safe
- all passwords are required to be a minimum of 12 characters long
- the Systems Manager is responsible for ensuring that all software purchased by and used by the school is adequately licensed and that the latest software updates (patches) are applied
- the helpdesk (networkhelp@mggs.org) is used for reporting minor/non-urgent issues and support. Security breaches and cyber threat incident procedures are detailed in the Cyber Security Incident Management Plan
- appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems and devices from accidental or malicious attempts which might threaten the security of the school systems and data. These are tested regularly. The school infrastructure and individual workstations are protected by up-to-date endpoint (anti-virus) software
- supply and trainee teacher accounts are created in the same way as members of staff and subject to the same security levels. Visitors or guests are normally only given access to KIFI via a user specific username and password with an automatic expiry date
- staff are forbidden from downloading executable files and installing programmes on school devices. This can only be carried out by the Network Department
- all removable media (e.g., memory sticks/CDs/DVDs)are blocked on school devices. It can be approved on an individual basis for specific purposes
- external sharing via Google is blocked. Systems are in place to reduce the risk of sharing personal data with a large number of users

Mobile Technologies

The school acceptable use agreements for staff, students, parents, and carers outline the expectations around the use of mobile technologies.

Students in KS3 and KS4 are only to use school managed devices for online activity in school.

Students in KS5 (as of September 2025) are permitted to use personal devices such as tablets or laptops in line with the acceptable use agreement.

Students in Year 13 are currently permitted to use their mobile phones in line with the same agreement. This is being phased out for September 2025.

The school allows:

	School Devices			Personal Devices		
	School owned for individual use	School owned for multiple users	Authorised device[1]	Student owned	Staff owned	Visitor owned
Allowed in school	Yes	Yes	Yes	Yes - KS3/KS4 in locked pouch. KS5 - yes	Yes/	Yes/
Full network access	Yes	Yes	Yes	KS5 Tablets or laptops only	Yes, in line with school log in access	No
Internet only						Yes
No network access						

Social Media

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

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

School staff should ensure that within their personal social media accounts:

- no reference should be made in social media to learners, parents/carers or school staff
- they do not engage in online discussion on personal matters relating to members of the school community
- personal opinions should not be attributed to the school
- security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information
- they act as positive role models in their use of social media

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

- a process for approval by senior leaders

[1] Authorised device – purchased by the learner/family through a school-organised scheme. This device may be given full access to the network as if it were owned by the school.

- clear processes for the administration, moderation, and monitoring of these accounts – involving at least two members of staff
- a code of behaviour for users of the accounts
- School social media channels will be managed by dedicated school accounts and not linked to staff personal accounts
- systems for reporting and dealing with abuse and misuse
- understanding of how incidents may be dealt with under school disciplinary procedures

Personal Use

- personal communications are those made via personal social media accounts. In all cases, where a personal account is used which associates itself with, or impacts on, the school it must be made clear that the member of staff is not communicating on behalf of the school with an appropriate disclaimer. Such personal communications are within the scope of this policy
- personal communications which do not refer to or impact upon the school are outside the scope of this policy
- where excessive personal use of social media in school is suspected, and considered to be interfering with relevant duties, disciplinary action may be taken

Monitoring of Public Social Media

- As part of active social media engagement, the school may pro-actively monitor the Internet for public postings about the school
- the school should effectively respond to social media comments made by others according to a defined policy or process
- when parents/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

Digital and 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

- staff must obtain permission from a member of the leadership team before using live-streaming or video-conferencing services with students. Any use must be in line with national and local safeguarding guidance / policies
- when using digital images, staff will inform and educate learners about the risks associated with the taking, use, sharing, publication and distribution of images
- staff/volunteers must be aware of those learners 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
- staff and volunteers are allowed to take digital/video images to support educational aims, but must follow school policies concerning the sharing, storage, distribution and publication of those images
- care should be taken when sharing digital/video images that learners are appropriately dressed
- learners must not take, use, share, publish or distribute images of others without their permission

- photographs published on the website, or elsewhere that include learners will be selected carefully and will comply with the Online Safety Policy
- learners' full names will not be used anywhere on a website or blog, particularly in association with photographs
- written permission from parents or carers will be obtained before photographs of learners are taken for use in school or published on the school website/social media.
- parents/carers will be informed 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
- images will be securely stored in line with the school retention policy

Online Publishing

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

- Public-facing website
- Social media
- Online newsletters

The school website is managed internally and hosted by Ionos. 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 student work, images or videos are published, their identities are protected, and full names are not published.

The website includes an online reporting process for parents and the wider community to register safeguarding and bullying concerns to complement the internal reporting process.

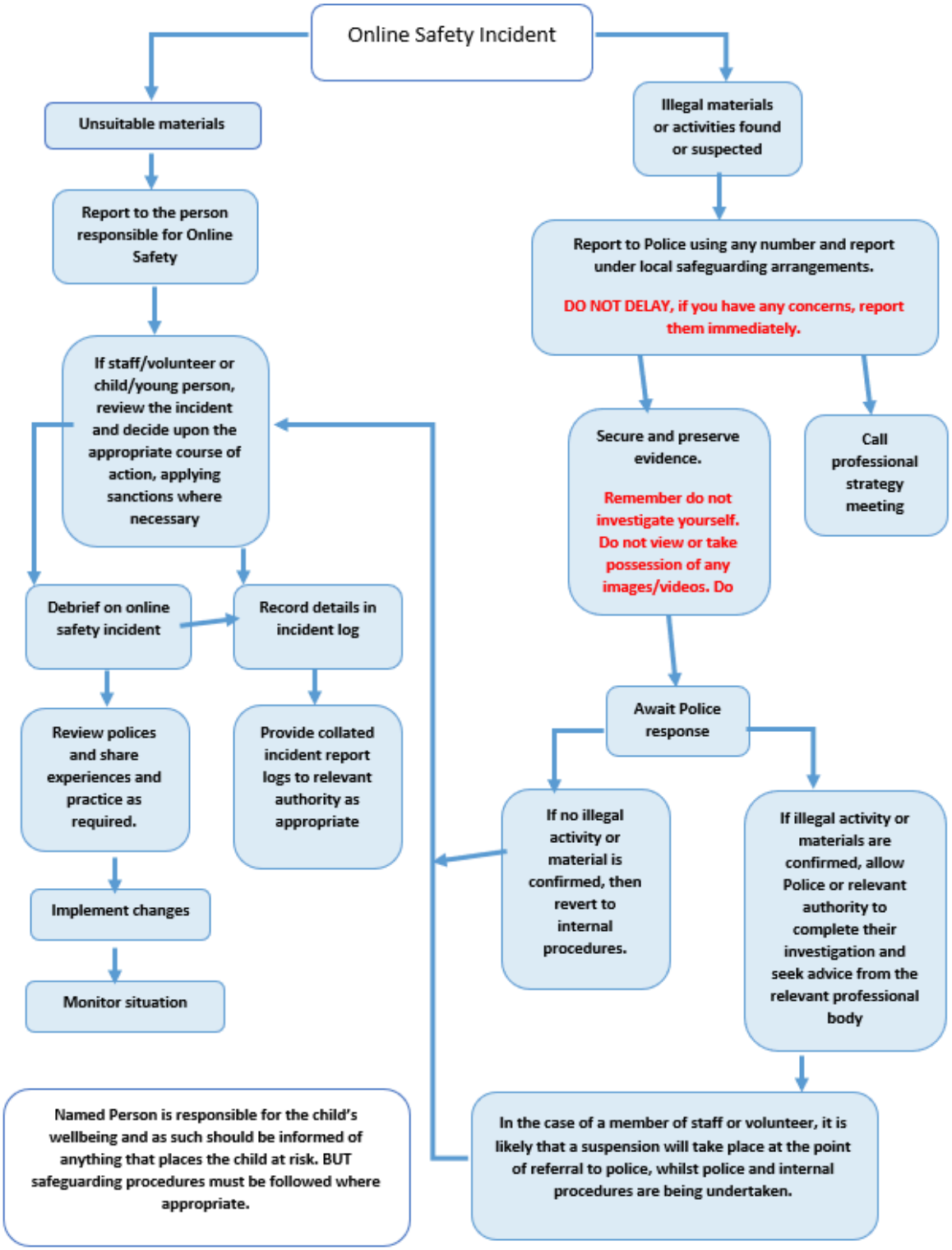
Data Protection

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

Appendices

Responding to incidents of misuse flow chart
Links to other organisations and resources
Glossary of Terms

Responding to incidents of misuse – flow chart



Links to other organisations or documents

The following links may help those who are developing or reviewing a school online safety policy and creating their online safety provision:

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

Glossary of Terms

AUP/AUA	Acceptable Use Policy/Agreement – see templates earlier in this document
CEOP	Child Exploitation and Online Protection Centre (part of National Crime Agency, UK Police, dedicated to protecting children from sexual abuse, providers of the Think U Know programmes.
CPD	Continuous Professional Development
FOSI	Family Online Safety Institute
ICO	Information Commissioner's Office
ICT	Information and Communications Technology
INSET	In Service Education and Training
IP address	The label that identifies each computer to other computers using the IP (internet protocol)
ISP	Internet Service Provider
ISPA	Internet Service Providers' Association
IWF	Internet Watch Foundation
LA	Local Authority
LAN	Local Area Network
MAT	Multi Academy Trust
MIS	Management Information System
NEN	National Education Network – works with the Regional Broadband Consortia (e.g. SWGfL) to provide 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