Online Safety Policy

Adapted from the Local Authority Model (May 2018)

& SWGFL School Online Safety Policy (2022) / The Key (2023)

Signed (chair):	**Name:** Donna Whinham	**Date:** 16.11.23
Signed (Head):	**Name:** Tracy Serle	**Date:** 16.11.23
Reviewed by: S McSmythurs	**Reviewed on:** 7/11/23	**Note of Revisions:** June 2018 – inclusion of reference to smart watches. January 2021: Managing incidents diagram update, KCSIE 3Cs; Prevent; Remote learning; Managing sexting incidents; September 2022: Significant revision to all areas: all diagrams, tables, information on personal devices and mobile technologies, BHJS online education programme, roles and responsibilities and online publishing sections to reflect KCSIE 2022. November 2023: Updates to Governor/Senior Leader Roles and Responsibilities in Appendix 1 Artificial Intelligence: updated table (Page 8) and new paragraph (Page 12)
Ratified by: **Governing Body on**		**Next Review:** October 2024

Equality Impact Assessment (EIA) Part 1: EIA Screening

Policies, Procedures or Practices	Online -Safety	Date	15/11/2
EIA CARRIED OUT BY:	T.Serle	EIA APPROVED BY:	T Serle

Groups that may be affected:

Are there any concerns that the policy could have a different impact on any of the following groups? (please tick the relevant boxes)	Existing or potential adverse impact	Existing or potential for positive impact
Age (young people, the elderly: issues surrounding protection and welfare, recruitment, training, pay, promotion)		X
Disability (physical and mental disability, learning difficulties; issues surrounding access to buildings, curriculum and communication).		X
Gender Reassignment (transsexual)		X
Marriage and civil partnership		X
Pregnancy and maternity		N/A
Racial Groups (consider: language, culture, ethnicity including gypsy/traveller groups and asylum seekers		X
Religion or belief (practices of worship, religious or cultural observance, including non-belief)		X
Gender (male, female)		X
Sexual orientation (gay, lesbian, bisexual; actual or perceived)		X

Any adverse impacts are explored in a Full Impact Assessment.

Online Safety Policy

This Online safety policy has been developed by our Computing subject leader and will be reviewed and monitored by our school online safety working group which comprises of:

- Headteacher
- A representative of teaching staff and support staff
- A governor representative and a parent representative

Breadth of issues
The breadth of issues classified within online safety is considerable, but can be categorised into three areas of risk:

- **content**: being exposed to illegal, inappropriate or harmful material; for example pornography, fake news, racist or radical and extremist views;
- **contact:** being subjected to harmful online interaction with other users; for example commercial advertising as well as adults posing as children or young adults; and
- **conduct**: personal online behaviour that increases the likelihood of, or causes, harm; for example making, sending and receiving explicit images, or online bullying.
- **commerce**: risks such as online gambling, inappropriate advertising, phishing and or financial scams

KCSIE, 2022

Monitoring

The school will monitor the impact of the policy through an analysis of:

- Logs of reported incidents and responses
- Monitoring logs of internet activity and any network monitoring data
- Surveys / questionnaires of students, parents / carers, and staff including non-teaching staff
- Monitoring information about the teaching programme and coverage within the curriculum
- Regularly checking that pupils and staff are clear about how to report incidents and respond to them
- The content of the web site, Google Classroom, You Tube channel and twitter account is regularly monitored by governors and senior leaders to ensure that it complies with this policy and the acceptable use policies.

Scope of the Policy

This Online Safety Policy applies to all members of the school community (including staff, learners, 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 Education and Inspections Act 2006 empowers Head teachers, to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is relevant to incidents, including cyber-bullying, which may take place out of school, but are linked to membership of the school. The school will deal with

such incidents within this policy and associated behaviour and anti-bullying policies and will, inform parents / carers of known incidents of inappropriate online safety behaviour that take place out of school. The 2011 Education Act increased these powers with regard to searching for and of electronic devices and the deletion of data and related action can only be taken over issues covered by the school behaviour policy. When dealing with online safety issues, electronic devices will only be searched and data deleted with parents. If parents are unavailable the device will be kept securely until a parent can meet to conduct such a search with a senior leader.

This policy should be read alongside the acceptable use policies for staff and pupils, the anti-bullying policy and the behaviour policy.

Roles and Responsibilities

These are clearly detailed in Appendix 1 for all members of the school community.

- The Headteacher is responsible for ensuring the safety (including online safety) of members of the school community, though the day to day responsibility for online safety is delegated to the online safety Leader. The Headteacher is also the designated person for child protection and is trained in online safety issues and aware of the potential for serious child protection issues to arise from sharing of personal data, access to illegal / inappropriate materials, inappropriate on-line contact with adults / strangers, potential or actual incidents of grooming and cyber-bullying.
- The governing body monitors appropriate policies and procedures in place in order to safeguard and promote online safety. (KCSIE 2023) This is delegated to the Standards and Curriculum committee and the Online Safety Group.

Acceptable use

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

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

- Pupil acceptable use agreement
- Staff induction
- Staff handbook
- Posters/notices around where technology is used
- Communication with parents/carers
- Built into education sessions
- School website
- Peer support
- Email updates
- Newsletter updates to families

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

User actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Users shall not access online content (including apps, games, sites) to make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	**Any illegal activity for example:** • Child sexual abuse imagery* • Child sexual abuse/exploitation/grooming • Terrorism • Encouraging or assisting suicide • Offences relating to sexual images i.e., revenge and extreme pornography • Incitement to and threats of violence • Hate crime • Public order offences - harassment and stalking • Drug-related offences • Weapons / firearms offences • Fraud and financial crime including money laundering N.B. Schools should refer to guidance about dealing with self-generated images/sexting – UKSIC Responding to and managing sexting incidents and UKCIS – Sexting in schools and colleges					X
Users shall not undertake activities that might be classed as cyber-crime under the Computer Misuse Act (1990)	• Using another individual's username or ID and password to access data, a program, or parts of a system that the user is not authorised to access (even if the initial access is authorised) • Gaining unauthorised access to school networks, data and files, through the use of computers/devices • Creating or propagating computer viruses or other harmful files • Revealing or publicising confidential or proprietary information (e.g., financial / personal information, databases, computer / network access codes and passwords) • Disable/Impair/Disrupt network functionality through the use of computers/devices • Using penetration testing equipment (without relevant permission) N.B. Schools will need to decide whether these should be dealt with internally or by the police. Serious or repeat offences should be reported to the police. Under the Cyber-Prevent agenda the National Crime Agency has a remit to prevent learners becoming involved in cyber-crime and harness their activity in positive ways – further information here					X
Users shall not undertake activities that are not illegal but are classed as unacceptable in school policies:	Accessing inappropriate material/activities online in a school setting including pornography, gambling, drugs. (Informed by the school's filtering practices and/or AUAs)			X	X	
	Promotion of any kind of discrimination				X	

User actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
	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	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 & other adults				Students / Pupils			
Communication Technologies	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission	Not allowed
Online gaming (educational)	x				x			
Online gaming (non-educational)				x				x
Online shopping / commerce			x					x
File sharing		x						x
Social Media		x						x
Messaging / Chat		x						x
Entertainment Streaming		x						x
Use of video broadcasting		x						x
Mobile phones may be brought to school	x						x	
Smart watches may be brought to school	x							x
Smart watches used in lessons				x				x
Use of mobile phones in lessons				x				x
Use of mobile phones in social time	x							x
Taking photos on personal mobile phones or other camera devices				x			x	
Taking photos on school cameras	x						x	
Use of hand held devices eg PDAs				x				x
Use of personal email addresses in school, or on school network				x				x
Use of school email for personal emails				x				x
Use of messaging apps			x					x
Use of wider social media				x				x
Use of blogs		x					x	
Use of X (Twitter)	x							x
Staff publishing content (YouTube)		x						x
Use of video conferencing (remote learning)		x				x		

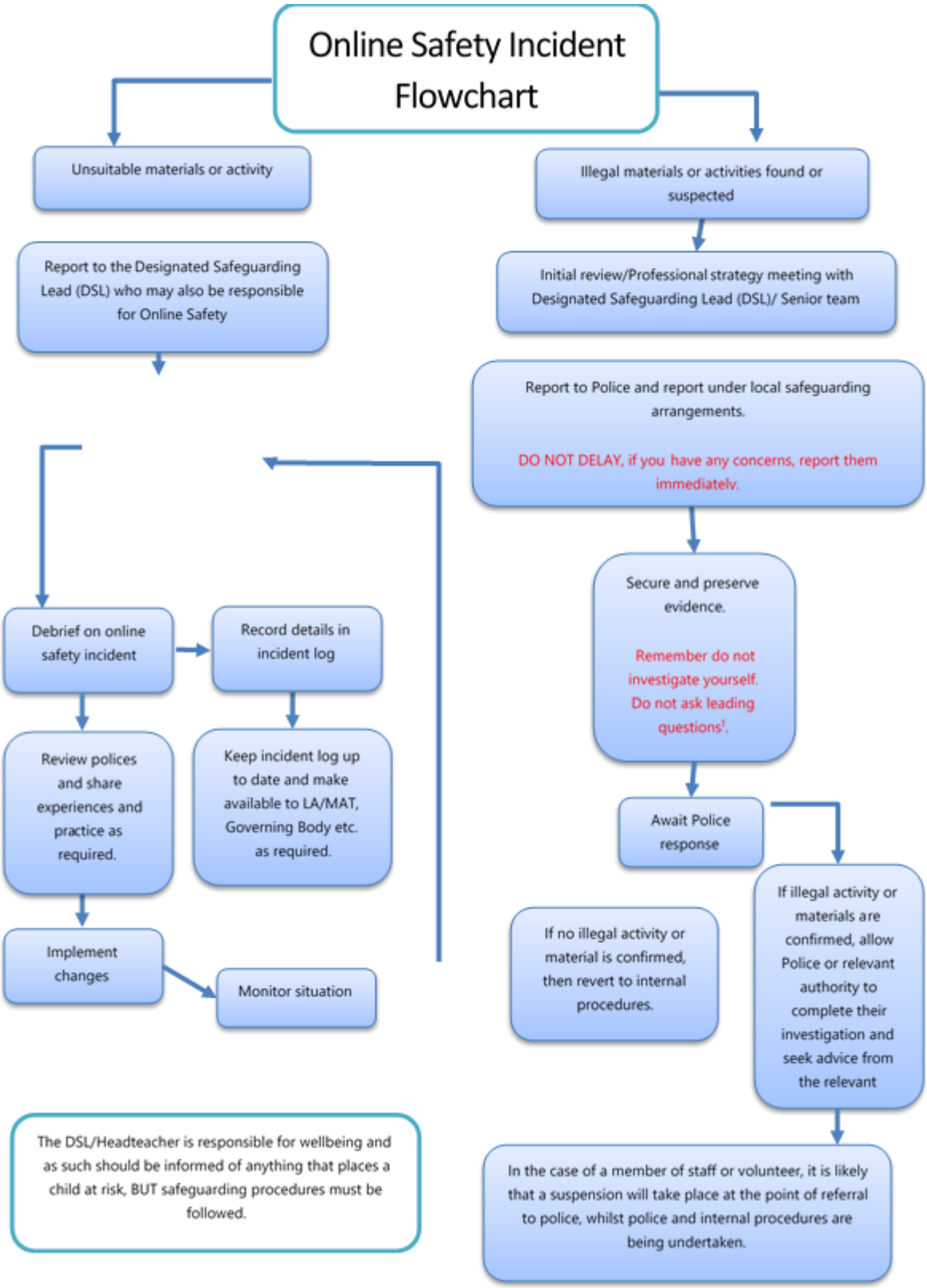
Use of Artificial Intelligence (ChatGPT, TeachAI, Google Bard, Oak AI)	x							x

Reporting and Responding

- All members of the school community will be made aware of the need to report online safety issues/incidents which are consistent with the school safeguarding procedures, and with the whistleblowing, complaints and managing allegations policies.
- Reports on CPOMS / paper safeguarding form 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 (see flowchart and user actions chart in the appendix), 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 and the local authority / MAT
- where there is no suspected illegal activity, devices may be checked using the following procedures:
    - one or more senior members of staff should be involved in this process. This is vital to protect individuals if accusations are subsequently reported.
    - conduct the procedure using a designated device that will not be used by 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
        - involvement by local authority / LADO
        - 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 using CPOMS

- Relevant staff are aware of external sources of support and guidance in dealing with online safety issues, e.g. local authority; police; Professionals Online Safety Helpline; Reporting Harmful Content; CEOP.
- Those involved in the incident will be provided with feedback about the outcome of the investigation and follow up actions (as relevant)
- Learning from the incident (or pattern of incidents) will be provided to:
    - *the Online Safety Group for consideration of updates to policies or education programmes and to review how effectively the report was dealt with*
    - *staff, through regular briefings*
    - *learners, 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.



Staff should report online safety issues using CPOMs to the Online Safety Lead and Headteacher. If these include allegations of bullying then the anti-bullying policy is followed. Issues which may impact on the well-being and safety of a child are reported directly to the Child Protection Lead and Child Protection procedures are followed. Issues impacting on staff or to the detriment of the school should be reported to the headteacher or to the Chair of Governors if the headteacher is absent or the accusation involves the headteacher.

Pupils are encouraged to report any incidents to an adult whether it relates to themselves or a friend. We encourage children to take responsibility for protecting each other.

Artificial intelligence (AI)

Generative artificial intelligence (AI) tools are now widespread and easy to access. Staff, pupils and parents/carers may be familiar with generative chatbots such as ChatGPT and Google Bard.

BHJS recognises that AI has many uses to help pupils learn, but may also have the potential to be used to bully others. For example, in the form of 'deepfakes', where AI is used to create images, audio or video hoaxes that look real.

BHJS will treat any use of AI to bully pupils in line with our behaviour and antibullying policy.

Staff should be aware of the risks of using AI tools whilst they are still being developed and view the Online Safety Risk Assessment regarding new AI tools.

Managing Incidents

This guidance is intended for use when staff need to manage incidents that involve the use of online services. It encourages a safe and secure approach to the management of the incident. Incidents might involve illegal or inappropriate activities.

Illegal Incidents

If there is any suspicion that the web site(s) concerned may contain child abuse images, or if there is any other suspected illegal activity, refer to the right hand side of the Flowchart for responding to online safety incidents and report immediately to the police.

Responding to Learners Action

Incidents	Refer to class teacher/tutor	Refer to Online Safety Lead	Refer to Headteacher	Refer to Police/Social Work	Refer to local authority technical support for advice/action	Inform parents/carers	Remove device/ network/internet access rights	Issue a warning	Further sanction, in line with behaviour policy
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on User Actions on unsuitable/inappropriate activities).		X	X	X					
Attempting to access or accessing the school network, using another user's account (staff or learner) or allowing others to access school network by sharing username and passwords	X	X				X	X	X	
Corrupting or destroying the data of other users.			X			X		X	X
Sending an e-mail, text or message that is regarded as offensive, harassment or of a bullying nature			X			X		X	
Unauthorised downloading or uploading of files or use of file sharing.		X	X		X	X			
Using proxy sites or other means to subvert the school's filtering system.			X		X	X			
Accidentally accessing offensive or pornographic material and failing to report the incident.			X		X	X			
Deliberately accessing or trying to access offensive or pornographic material.			X			X			X
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act.		X				X			
Unauthorised use of digital devices (including taking images)	X	X				X			

Unauthorised use of online services	x	x				x			
Actions which could bring the school into disrepute or breach the integrity or the ethos of the school.			x		x	x			
Continued infringements of the above, following previous warnings or sanctions.	x	x	x		x	x			x

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

Actions which could compromise the staff member's professional standing	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
Failing to report incidents whether caused by deliberate or accidental actions	x	x	X			x	x	x
Continued infringements of the above, following previous warnings or sanctions.	x	x	X				x	x

- More than one senior member of staff should be involved in investigating to protect possible future accusations.
- Use a computer that will not be used by young people which could be taken off site by the police if required.
- Ensure staff have internet access to investigate but that sites and content are closely monitored and recorded.
- Record the URL of any site containing alleged misuse and the nature of the content causing concern. It may be useful to record and store screenshots of the content by printing them, signing them and attaching them to the record. Except for child abuse images as this would constitute an offence.
- Once the investigation is complete the investigating group should identify the appropriate response in line with policies which may internal procedures, involvement of LA or police.

Reporting to the police

- If the content being reviewed includes images of child abuse then monitoring should be stopped and the police informed immediately. Other incidents to be referred to the police are
    - incidents of 'grooming' behaviour
    - the sending of obscene materials to a child
    - adult material which potentially breaches the Obscene Publications Act
    - criminally racist material
    - promotion of terrorism or extremism
    - other criminal conduct, activity or materials

  In any of the above, isolate the computer involved as any change to its stage may hamper a police investigation.

If issues could be a result of problems with infrastructure or may affect it then the technical support provider is informed immediately (for South Gloucestershire support 3838).

If access to an unsuitable site is reported then the Online Safety lead will alert the technical support team by ringing 3838 to ensure that this is blocked. Serious incidents are escalated to local authority staff for advice and guidance.

Nick Pearce – infrastructure, technical and filtering – 01454 86**3838**

Jo Briscombe – curriculum and policy – 01454 86**3349**

Tina Wilson – LADO allegations against staff and volunteers – 01454 86**8508**

Access and response team (ART) – safeguarding / child protection concerns **-** 01454 86**6000** (Monday to Friday) and 01454 615165 (Out of hours/Weekends)

Arbor: Primary School Support – 020 8050 2086

E-Limelight (Website Provider / Host) – Clare Lester, 0117 214 0167 www.elimelight.co.uk

For incidents affecting school staff the Professionals Online Safety Helpline is contacted for advice if necessary on helpline@saferinternet.org.uk or 0844 381 4772.

Any reported incidents are logged in the CPOMs and followed up in accordance with the relevant policy depending on the issue. The response is also logged and serious issues are followed up after an interval of time to ensure that they are fully resolved.

Where appropriate school newsletters and the website are used to provide guidance to staff following an incident in order to prevent further incidents happening.

Managing Incidents of Youth Produced Sexual Imagery (Sexting)

In the latest advice for schools and colleges (UKCIS, 2020), this is defined as the sending or posting of nude or semi-nude images, videos or live streams online by young people under the age of 18. This could be via social media, gaming platforms, chat apps or forums. It could also involve sharing between devices via services like Apple's AirDrop which works offline. Alternative terms used by children and young people may include 'dick pics' or 'pics'.

The motivations for taking and sharing nude and semi-nude images, videos and live streams are not always sexually or criminally motivated.

This advice does not apply to adults sharing nudes or semi-nudes of under 18-year olds. This is a form of child sexual abuse and must be referred to the police as a matter of urgency (as outlined above).

DfE guidance for staff (2020)

- **Never** view, copy, print, share, store or save the imagery yourself, or ask a child to share or download – **this is illegal**.
- If you have already viewed the imagery by accident (e.g. if a young person has showed it to you before you could ask them not to), report this to the DSL (or equivalent) and seek support.
- **Do not** delete the imagery or ask the young person to delete it.
- **Do not** ask the child/children or young person(s) who are involved in the incident to disclose information regarding the imagery. This is the responsibility of the DSL (or equivalent).
- **Do not** share information about the incident with other members of staff, the young person(s) it involves or their, or other, parents and/or carers.
- **Do not** say or do anything to blame or shame any young people involved.
- **Do** explain to them that you need to report it and reassure them that they will receive support and help from the DSL (or equivalent).

Online Safety Education Programme

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

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 (statements may need to be adapted, depending on school structure and the age of the learners).

- 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 regularly taught in a variety of contexts. This will use Project Evolve and Google Be Internet Legends
- Lessons are matched to need; are age-related and build on prior learning

- Strands included in Project Evolve are: Internet safety Privacy and security; Relationships and communication; Cyberbullying; Information literacy; Self-image and identity; Digital footprint and reputation; Creative credit and copyright
- Strands included in Google's Be Internet Legends: Sharp, Alert, Secure, Kind, Brave.
- Lessons are context-relevant with agreed objectives leading to clear and evidenced outcomes
- Digital competency is planned and effectively threaded through the appropriate digital discussion in other curriculum areas e.g. PHSE; SRE; Literacy etc
- Our curriculum incorporates/makes use of relevant national initiatives and opportunities e.g. Safer Internet Day and Anti-bullying week
- The programme will be accessible to learners at different ages and abilities such as those with additional learning needs or those with English as an additional language.
- Pupils should be helped to understand the need for the learner acceptable use agreement and encouraged to adopt safe and responsible use both within and outside school
- Staff should act as good role models in their use of digital technologies the internet and mobile devices
- In lessons where internet use is pre-planned, it is best practice that 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 learners are allowed to search the internet around a topic – they should use Swiggle (child search engine from SWGFL) or agreed websites signposted by the teacher. Staff should be vigilant in supervising the learners and monitoring the content of the websites the young people visit
- If particular websites or recommended apps are blocked by the filtering system, staff can request via the head teacher for this block to be removed by Integra IT, pending research of alternative approved apps and discussion with Integra IT.

Contribution of Learners

The school acknowledges, learns from, and uses the skills and knowledge of learners 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:

- *the Online Safety Group has learner representation through school council*
- *learners contribute to the online safety education programme e.g. online safety campaigns*
- *contributing to online safety events with the wider school community e.g. parents' evenings, family learning programmes etc.*

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/group involved in technology/online safety/health and safety/safeguarding. This may be offered in several ways such as:

- attendance at training provided by the local authority or NSPCC
- 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

Many parents and carers have only a limited understanding of online safety risks and issues, yet they play an essential role in the education of their children and in the monitoring/regulation of the children's online behaviours. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.

The school will seek to provide information and awareness to parents and 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 awareness workshops / parent/carer evenings etc*
- *the learners – who are encouraged to pass on to parents the online safety messages they have learned in lessons and by learners leading sessions at parent/carer evenings.*
- *letters, newsletters, website, learning platform,*
- *high profile events / campaigns e.g. Safer Internet Day*
- *reference to the relevant web sites/publications*
- *Sharing good practice with other schools*

Adults and Agencies

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

- online safety messages targeted towards families and relatives.
- providing family learning courses in use of digital technologies and online safety
- the school will provide online safety information via their website and social media for the wider community

- work with Bromley Heath Infant to enhance online safety provision in wider community

Online Learning

Online learning will take place using the Google Classroom platform as part of routine homework. Staff will receive relevant CPD and regularly review systems to ensure Google Classroom platform is used effectively to facilitate home learning. Children will be regularly reminded of the acceptable use policy and online safety messages.

- Staff will use work provided equipment where possible e.g. a school/setting laptop, tablet or other device for safeguarding purposes and data security e.g. using strong passwords, suitable levels of encryption, logging off or locking devices when not in use etc.

- To report any problems or mis-use as set out in this policy, children are able to privately message their teacher, and parents can email teachers directly. Teachers will then need to record instances on CPOMs and/or using our behaviour policies.

Rules for Keeping Safe

These are reinforced through the following:

- Pupils sign an acceptable use agreement and this is also communicated to parents who we hope will reinforce the messages at home.
- Pupils are helped to understand the student acceptable use policy and school rules for online safety and encouraged to act accordingly.
- All classes share the online safety rules annually regularly refer to these, for example, during activities where children are searching the internet for information.
- Staff act as good role models in their own use of ICT.
- Staff are aware that there may be some children that are more vulnerable than others to being approached online and endeavour to ensure that these children understand the issues involved.
- Online behaviour is dealt with in accordance with our behaviour policy. There are sanctions and rewards in place for this.

Self-evaluation and Improvement

The school undertakes self-evaluation in order to inform actions to continually improve online safety provision through the following:

- Local authority safeguarding audit
- Surveys with pupils and staff
- 360Safe Review Tool

Technical Issues

The local authority provides technical and curriculum guidance for Online safety issues for **all** South Gloucestershire schools as well as providing direct technical support to a large number of schools.

Arbor provides technical support for the Management Information System

E-Limelight provides support for the school website.

Head teacher (as DSL) and Deputy Head teacher/SENCO (as DDSL) are able to manage content for Twitter.

Password Access to Systems

All our systems are accessed via an individual log in. Users have passwords that include upper and lower case and a number and are encouraged to change these regularly. **Users are told that passwords must never be shared for any IT system and that they are responsible for any actions taking using their log in**.

Staff users are required to set up two-factor authentication to use South Glos school systems – e.g. email and remote access to the virtual server drive.

Integra IT provides an always on Virtual Private Network – that operates both in school and at home on staff laptops.

Internet Provider and Filtering

The South Gloucestershire school internet service is provided by Integra and this includes a filtering service to limit access to unacceptable material for all users.

Internet access is filtered for all users by South Gloucestershire School IT. Illegal content (child sexual abuse images) is filtered by actively employing the Internet Watch Foundation CAIC list. Content lists are regularly updated and internet use is logged and regularly monitored.

The strict filtering of content prevents children from accessing internet chat rooms or web pages where radical or terrorist extremist material is could be encountered. N.B. additional duties for schools/academies under the Counter Terrorism and Securities Act 2015 which requires schools to ensure that children are safe from terrorist and extremist material on the internet.

However we are aware that no filtering is completely infallible and consequently focus on teaching pupils to keep safe through our curriculum and teaching. There are two different levels of filtering which are targeted towards different user groups. As a consequence teacher and staff users have access to some resources for teaching that are filtered for learners so as to ensure that "over blocking" does not restrict teaching.

Monitoring

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

- Integra IT Service Desk monitors all network use across all its devices and services.
- An appropriate monitoring strategy for all users has been agreed and users are aware that the network is monitored. Integra IT manage the monitoring system and alert the headteacher and online safety lead in instances of misuse.
- 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 strategy informed by the school's risk assessment which includes:

- physical monitoring (adult supervision in the classroom)

- internet use is logged, regularly monitored and reviewed
- filtering logs are regularly analysed and breaches are reported to senior leaders
- Pro-active alerts inform the school of breaches to the filtering policy, allowing effective intervention.
- where possible, school technical staff regularly monitor and record the activity of users on the school technical systems

The school reports issues through logging a call to the service desk at 3838 or emailing: servicedesk@integra.co.uk

Any filtering requests for change and issues are also reported immediately to the South Gloucestershire technical team on 3838. Technical issues relating to Arbor (Information Management System) this will be managed by the School Business Manager, Head teacher or Online Safety Lead.

Requests from staff for sites to be removed from the filtered list must be approved by the Headteacher and this is logged and documented by a process that is agreed by the Headteacher.

Technical Staff - Roles and Responsibilities

Where the local authority provides technical support the "administrator" passwords for the school are not held by the school and the local authority are responsible for their security and any implications of their use.

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

- There are regular reviews and audits of the safety and security of school ICT systems.
- Servers, wireless systems and cabling are securely located and physical access is restricted.
- All users have clearly defined access rights to school ICT systems and are provided with a username and password by the technical support provider.
- Users are responsible for the security of their username and password, must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security.
- An agreed policy is in place (to be described) for the provision of temporary access of "guests" (e.g. trainee teachers, visitors) onto the school system.
- School ICT technical staff regularly monitor and record the activity of users on the school ICT systems and users are made aware of this in the Acceptable Use Policy.
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations etc. from accidental or malicious attempts which might threaten the security of the school systems and data.
- The school infrastructure and individual workstations are protected by up to date virus software.
- An agreed policy is in place (Staff Handbook and Code of Conduct) regarding the extent of personal use that users (staff / students / pupils / community users) and their family members are allowed on laptops and other portable devices that may be used out of school.
- An agreed policy is in place that forbids staff from installing programmes on school workstations / portable devices.
- An agreed policy is detailed regarding the use of removable media (e.g. memory sticks / CDs / DVDs) by users on school workstations / portable devices in our acceptable use agreement.
- Guest Wi-Fi access is provided through temporary log ins using school equipment only. Passwords expire daily at 4pm.

Mobile technologies

The use of personal devices or smart watches is prohibited for pupils in school (with exception for medical conditions). They may only have their mobile device in school with permission from parent/carer as per mobile phone policy and stored in designated safe in classroom.

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

The school allows:

	Personal devices		
	Student owned	Staff owned	Visitor owned
Allowed in school	Yes (by agreement for medical / storage in day)	Yes (adhere to acceptable use)	Yes* (adhere to visitor acceptable use)
Full network access	No	No	No
Internet only	No	No	No
No network access	Yes	Yes	Yes
4G / 5G connectivity	4G / 5G use only by agreement for medical monitoring	In staffroom or out of hours when children not present	DBS checked Governors during out of hours meetings only

Personal devices

These might include mobile phones, tablets or any other device that has the capability of accessing the school's wireless network. The primary use of these in school is to support learning, teaching and management.

Staff and governors are unable to access Wi-Fi in school on their personal devices.

Children are not allowed to use their personal devices in school as the school provides access to the technologies to be used for learning.

Staff are not allowed to use their personal mobile phones in school while they are teaching and any use should be restricted to times when children are not present. The only exception to this is in case of emergency during a school trip.

Staff do not use their own mobile phone to take images of children or store any data relating to children (e.g. attachments from email), for example, on a school trip as the school has devices available for this.

Visiting peripatetic teachers are allowed to use South Glos device to support of learning, however no internet or system access will be provided

Any presenters should email the presentation in advance for school evaluation of material.

Supply code logins and use of school devices provided in staff absence. Codes expire daily.

Pupil Devices

- Individual pupils with medical conditions have a mobile phone linked to their diabetic monitoring
- The use of the 'Dexcom' app is the only use for the device in school (both by pupil and staff)
- Devices are protected by a PIN known by pupil and staff
- Staff work with families to ensure that they device is only used for this singular purpose by the pupil – particularly to promote independent.
- As these devices are connected to 4G the use of the pin is essential, and should never be shared with peers.
- Devices to be kept on the teacher's desk (for audio alarms linked to the app) OR with the child in playground during breaks
- Any misuse of this device will be immediately reported to head teacher and families.

School owned/provided devices (iPads):

- *Will be allocated to the year group using the Asset Register and regularly audited and checked by Integra IT and School Business Manager*
- *Personal use is not allowed as per the staff handbook*
- *Levels of access to networks/internet – iPads are filtered, with staff able to login to SGCYP website to release access to access Twitter*
- *Integra IT have full management of devices/installation of apps/changing of settings/iOS updates and monitoring*
- *Technical support provided by Integra IT*
- *Use on trips/events away from school is authorised for photos etc.*
- *Data protection: no pupil data to be stored directly on class iPads;*
- *Arbor login is available to cloud based service, staff to log in and out as required (to access registers for clubs).*
- *Taking of images is authorised, and images should then be deleted / stored on the Teacher Drive.*
- *No images should be kept for prolonged periods of time on the device.*
- *Exit processes – devices returned if staff member leaves / checked at end of year / regular audit*

Use of Digital Images and Video

Ease of access to technologies which take digital images and video has many benefits for learning. Taking and sharing images and video are much easier and, if not managed, this could increase the potential risk of misuse and has the potential to be used for cyberbullying. The school informs and educates users about the risks associated with digital images and these are outlined in the acceptable use policies:

- The school may use live-streaming or video-conferencing services to enhance education such as trips. Staff to follow guidance on remote learning, and risk assess the event as per other school trips. All links should be posted to school diary and through authorised work email accounts only.
- When using digital images, staff will inform and educate learners about the risks associated with the taking, use, sharing, publication and distribution of images.
- Pupils should not take, use, share, publish or distribute images / video of others without their permission and staff reinforce this when appropriate.
- Written permission is obtained from parents or carers before photographs of pupils are taken. These photographs are only taken to be used for educational purposes or to promote achievements or the school.

- 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 are allowed to take digital / video images to support educational aims, but follow guidance in the acceptable use policy concerning the sharing, distribution and publication of those images.
- Staff sign permission forms to say that they allow their image to be used for promoting the school and are aware of the risks of this being copied.
- Images are only taken and used of individuals where there is a signed permission form in place.
- Pupils full names are not published on any online platform or school communication including the web site, newsletter or twitter feed. Photographs published anywhere that include pupils are carefully selected and not used in association with pupils' full names or other information that could identify them.
- Care is always taken to ensure that pupils are appropriately dressed if images are taken and that they are not participating in any activity which might bring individuals or the school into disrepute.
- In accordance with guidance from the Information Commissioner's Office, parents / carers are welcome to take videos and digital images of their children at school events for their own personal use as this is not covered by the General Data Protection Regulation. However in order to protect other children and respect privacy these images should not be published or made publicly available on social networking sites. Parents / carers should also not comment on any activities involving other pupils in the digital / video images. This is clearly detailed in our acceptable use policy for parents.
- Pupils' work is only published with the permission of pupils and parents / carers.

Online Publishing

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

- Public-facing website
- Social media (Twitter, local information boards)
- Online and emailed newsletters
- *Downend Voice and other news publications*

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

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

The school provides information about online safety e.g., publishing the schools Online Safety Policy and acceptable use agreements; curating latest advice and guidance; news articles etc., creating an online safety page on the school website.

The website includes email contact point for parents and the wider community to register issues and concerns to complement the internal reporting process.

Communications Technologies and Social Media

A wide range of communications technologies have the potential to enhance learning and management. The acceptable use agreements outline how these systems should be used.

- The official school email service is used for communications between staff, and with parents/carers and students as it provides an effective audit trail. Communications are always professional in tone and content.
- Users are made aware that email communications may be monitored and what to do if they receive an email that makes them feel uncomfortable, is offensive, threatening or bullying in nature through the acceptable use policies.
- Governor communications take place through governor school e-mail accounts. Personal or sensitive information is not e-mailed but can be accessed directly from the school.
- Personal email addresses, text messaging, public chat and social networking programmes are not be used for communications with parents/carers and children.
- The school uses Twitter to update parents on news and events and this is managed and monitored by SLT who approves users, content and monitors use of the account.
- Personal information is also not posted on the school website and only official email addresses are listed for members of staff. The web site is the responsibility of the School Business Manager.
- Guidance on personal use of social media and mobile devices is included in the staff, parent and pupil acceptable use policies including clear reporting mechanisms. Training is provided for staff and risks, reporting and issues around social networking forms part of the learning for pupils.
- Staff ensure that no reference is made in social media to pupils, parents or other staff and do not engage in online discussions on personal matters about any member of the school community
- Personal opinions are not attributed to the school
- Security settings on personal social media profiles are regularly checked to minimise risk
- Staff personal use of social media where it does not relate to the school is outside the scope of the policy but is should be made clear that the member of staff is not communicating on behalf of the school. If staff come across communications that might bring the school into disrepute in their personal communications they should not get involved, refer the publisher to relevant complaints procedures and report the issue.
- The online safety lead pro-actively monitors the Internet for postings about the school.

Unsuitable/inappropriate activities include:

Copyright

The School Business Manager is responsible for making sure that software licence audit is regularly updated and also making regular checks to ensure the number of software installations matches the licences held. Where there are insufficient licences this could breach the Copyright Act which may lead to fines or unexpected additional license costs.

Data Protection

Personal Data is defined as any data which relate to a living individual who can be identified from the data. This includes opinion about the individual. Sensitive Personal Data about a person includes information about their racial or ethnic origin, political opinions, their religious beliefs or other beliefs of a similar nature, whether they are a member of a trade union and their physical or mental health or condition.

Personal data is recorded, processed, transferred and made available according to the General Data Protection Regulation and is:

- Fairly and lawfully processed
- Processed for limited purposes
- Adequate, relevant and not excessive
- Accurate
- Kept no longer than is necessary
- Processed in accordance with the data subject's rights
- Secure and only transferred to others with adequate protection

Transfer of Data

Whenever possible secure online storage is used to ensure that documents do not need to be transferred to limit the risk. We ensure that data is stored in accordance with the requirements laid down by the Information Commissioner's Office and within the EU. This also applies to cloud storage used.

The school ensures that:

- It holds the minimum personal data necessary to enable it to perform its function and does not hold it for longer than necessary for the purposes it was collected for.
- The data held is accurate, up to date and inaccuracies are corrected as quickly as possible.
- All personal data is fairly obtained in accordance with our "Privacy Notice" and lawfully processed in accordance with the "Conditions for Processing" as outlined in the policy on the South Gloucestershire IMS Traded Services web site.
- Personal and sensitive data relating to pupils or staff is not e-mailed as this is not secure.
- Personal data including assessment data is transferred using secure file transfer.
- Where information does need to be transferred between devices then encrypted memory sticks are used.
- It has clear and understood arrangements for the security, storage and transfer of personal data
- It is registered as a Data Controller for the purposes of the General Data Protection Regulation (GDPR)
- There is a Senior Information Risk Officer (SIRO) and Information Asset Owner (IAOs) in place.
- Risk assessments are regularly carried out.
- Data subjects have a right to access their data and there are clear procedures for this.
- There are clear and understood policies and routines for the deletion and disposal of data.
- There is a policy for reporting, logging, managing and recovering from information risk incidents.

- There are clear Data Protection clauses in all contracts where personal data may be passed to third parties.
- Only cloud storage that meets the requirements laid down by the Information Commissioner's office is used to store personal data.
- The staff acceptable use policy clearly defines the data protection measures that staff should take and how data can be securely stored and deleted.

Staff ensure that they

- Take care to ensure safe keeping of personal data and minimise the risk or loss or misuse
- Use personal data only on secure password protected computers and devices and log off at the end of every session
- Transfer data using encryption and secure password protected devices

Where personal data is stored on removable media:

- The data is encrypted and password protected
- The device is password protected
- The device has approved virus and malware checking software
- The data is securely deleted from the device once finished with.

Appendix 1: Roles and Responsibilities

Role	Responsibility
Governors	The governing board has overall responsibility for monitoring this policy and holding the headteacher to account for its implementation. The governing board will make sure all staff undergo online safety training as part of child protection and safeguarding training, and ensure staff understand their expectations, roles and responsibilities around filtering and monitoring. The governing board will also make sure all staff receive regular online safety updates (via email, e-bulletins and staff meetings), as required and at least annually, to ensure they are continually provided with the relevant skills and knowledge to effectively safeguard children. The governing board will co-ordinate regular meetings with appropriate staff to discuss online safety, requirements for training, and monitor online safety logs as provided by the designated safeguarding lead (DSL). The governing board should ensure children are taught how to keep themselves and others safe, including keeping safe online. The governing board must ensure the school has appropriate filtering and monitoring systems in place on school devices and school networks, and will regularly review their effectiveness. The board will review the DfE filtering and monitoring standards, and discuss with IT staff and service providers what needs to be done to support the school in meeting those standards, which include: • Identifying and assigning roles and responsibilities to manage filtering and monitoring systems; • Reviewing filtering and monitoring provisions at least annually; • Blocking harmful and inappropriate content without unreasonably impacting teaching and learning; • Having effective monitoring strategies in place that meet their safeguarding The online safety governor will: o Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet o Ensure that online safety is a running and interrelated theme while devising and implementing their whole-school or college approach to safeguarding and related policies and/or procedures o Ensure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some pupils with special educational needs and/or disabilities (SEND). This is because of the importance of recognising that a 'one size fits all' approach may not be appropriate for all children in all situations, and a more personalised or contextualised approach may often be more suitable

Online Safety Group	Members of the Online Safety Group (including Online Safety Governor, DSL, Family Link Worker) will assist the Online Safety Lead with: • the production/review/monitoring of the school Online Safety Policy/documents • the production/review/monitoring of the school filtering policy (if possible and if the school chooses to have one) and requests for filtering changes • mapping and reviewing the online safety education provision – ensuring relevance, breadth and progression and coverage • reviewing network/filtering/monitoring/incident logs, where possible • encouraging the contribution of learners to staff awareness, emerging trends and the school online safety provision • consulting stakeholders – including staff/parents/carers about the online safety provision • monitoring improvement actions identified through use of the 360-degree safe self-review tool.
Head teacher and Senior Leaders:	The headteacher 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 may be delegated to the Online Safety Lead. o Ensure that staff understand this policy and that it is being implemented consistently throughout the school o Work with the governing board to review this policy annually and ensure the procedures and implementation are updated and reviewed regularly o Take the lead on understanding the filtering and monitoring systems and processes in place on school devices and school networks o Work with the ICT Technicians / Integra to make sure the appropriate systems and processes are in place o Working with ICT team and other staff, as necessary, to address any online safety issues or incidents o Manage all online safety issues and incidents in line with the school's child protection policy o Ensure that any online safety incidents are logged and dealt with appropriately in line with this policy o Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour policy o Update and deliver staff training on online safety o Liaise with other agencies and/or external services if necessary o Provide regular reports on online safety in school to the headteacher and/or governing board o Undertaking annual risk assessments that consider and reflect the risks children face o Provide regular safeguarding and child protection updates, including online safety, to all staff, at least annually, in order to continue to provide them with relevant skills and knowledge to safeguard effectively.

Online safety Leader:	• lead the Online Safety Group • work closely on a day-to-day basis with the Designated Safeguarding Lead (DSL), where these roles are not combined • 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 (school/local authority/MAT/external provider) 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 • attend relevant governing body meetings/groups • report regularly to headteacher/senior leadership team. • liaises with the local authority/MAT/relevant body.
Child Protection Safeguarding Lead	The Designated Safeguarding Lead should be trained in online safety issues and be aware of the potential for serious safeguarding issues to arise from: • sharing of personal data [1] • access to illegal/inappropriate materials • inappropriate online contact with adults/strangers • potential or actual incidents of grooming • online bullying.
Curriculum Leaders	Curriculum Leads will work with the Online Safety Lead to develop a planned and coordinated online safety education programme using Project EVOLVE . This will be provided through: • a discrete programme • PHSE and SRE programmes • A mapped cross-curricular programme • assemblies and pastoral programmes • through relevant national initiatives and opportunities e.g. Safer Internet Day and Anti-bullying week.

Teaching and Support Staff	Teaching and support staff are responsible for ensuring that: • they have an awareness of current online safety matters/trends and of the current school Online Safety Policy and practices • they understand that online safety is a core part of safeguarding • they have read, understood, and signed the staff acceptable use agreement (AUA) • they immediately report any suspected misuse or problem to *(Tracy Serle, DSL or Stewart McSmythurs DDSL)* for investigation/action, in line with the school safeguarding procedures • all digital communications with learners and parents/carers should be on a professional level *and only carried out using official school systems* • 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, have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations • they supervise and monitor the use of digital technologies, mobile devices, cameras, etc., in lessons and other school activities (where allowed) and implement current policies regarding these devices • in lessons where internet use is pre-planned 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.
Students / pupils	• are responsible for using the school digital technology systems in accordance with the learner acceptable use agreement and Online Safety Policy (this should include personal devices – where allowed) • should understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so • should know what to do if they or someone they know feels vulnerable when using online technology • should understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the school's Online Safety Policy covers their actions out of school, if related to their membership of the school.
Parents and carers	Read the school guidance about online safety in the newsletter and on the website and take appropriate action if required to keep their child safe. Endorse (by signature) the Pupil Acceptable Use Policy

	Ensure that their child / children follow appropriate acceptable use rules at home Discuss online safety issues with their child / children and monitor their home use of ICT systems (including mobile phones and games devices) and the internet Access the school website / online platform in accordance with the relevant school Acceptable Use Policy. Keep up to date with issues through school updates and attendance at events Ensure they follow the school policy on taking digital and video images at school events Ensure their children following rules on appropriate use of children's own devices in school Report any online safety issues that could impact on safeguarding of any children or learning in school so that the school can put in place appropriate measures and use these to inform any changes to teaching
Technical Support Provider	• 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/MAT 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 Tracy Serle / Stewart McSmythurs 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
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 AUP before being provided with access to school systems. *The school encourages the engagement of agencies/members of the community who can provide valuable contributions to the online safety provision and actively seeks to share its knowledge and good practice with other schools and the community.*