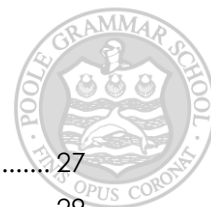


<b>Online Safety Policy</b>			
<b>Version</b>	<b>Date</b>	<b>Author</b>	<b>Review Date</b>
V1.00	September 2023	Mr N Chase	September 2024
<b>Authorised by:</b>		Dr A Smith	
<b>Ratified by:</b>		Full Governing Body	
<b>Date ratified:</b>		October 2023	

## Contents

1. Introduction.....	3
2. Scope of the Online Safety Policy .....	4
3. Policy development, monitoring and review .....	4
4. Roles & Responsibilities .....	5
5. Acceptable use .....	7
6. Reporting and Responding.....	11
7. Online Safety Education Programme .....	18
8. Education and Engagement of Staff/Volunteers.....	18
9. Education and Engagement of Parents/Carers.....	18
10. Technology .....	19
10.1 Filtering.....	19
10.2 Monitoring .....	20
10.3 Technical Security.....	21
10.4 Mobile technologies .....	22
10.4.1 Expectations for safe use of personal devices and mobile phones .....	22
10.4.2 Students use of personal devices and mobile phones.....	22
10.4.3 Staff use of personal devices and mobile phones .....	23
10.4.4 Visitors use of personal devices and mobile phones .....	24
10.5 Social Media.....	24
10.5.1 Official use of social media .....	24
10.5.2 Personal use.....	25
10.5.3 Students use of social media .....	26
10.5.4 Monitoring of public social media .....	26
10.6 Digital and Video Images .....	27



10.7	Online Publishing.....	27
11.	Appendix 1: Technology acceptable use agreement for students.....	29
11.1	For my own personal safety:.....	29
11.2	User Accounts .....	29
11.3	Use of Technology .....	29
11.4	Personal Devices.....	30
11.5	Social Media.....	30
11.6	Reporting Misuse .....	30
11.7	Agreement.....	30
12.	Appendix 2 – Technology acceptable use agreement for staff, governors, volunteers and guests .....	31
12.1	Definitions .....	31
12.2	User Accounts .....	31
12.3	Use of Technology .....	31
12.4	Personal Devices.....	31
12.5	Web and Social Media .....	32
12.6	Training.....	32
12.7	Reporting Misuse .....	32
12.8	Agreement.....	32
13.	Appendix 3 – Log sheets .....	33
13.1	Record of reviewing devices .....	33
13.2	Filtering change request .....	34
13.3	Online Safety Incident report form.....	35
13.4	Online Safety Incident Record.....	37
14.	Appendix 4 - Procedures for Responding to Specific Online Incidents or Concerns.....	40
14.1	Responding to concerns regarding Youth Produced Sexual Imagery ("Sexting") ....	40
14.2	Responding to concerns regarding Online Child Sexual Abuse and Exploitation (including child criminal exploitation) .....	41
14.3	Responding to concerns regarding Indecent Images of Children (IIOC) .....	41
14.4	Responding to concerns regarding radicalisation or extremism online .....	42
14.5	Responding to concerns regarding cyberbullying .....	42
14.6	Responding to concerns regarding Online Hate .....	43
15.	Appendix 5 - Equality Impact Assessment (EQIA) .....	44



## 1. Introduction

The internet, mobile and digital technologies are an important part of everyday life and provide positive opportunities for children and young people to learn, socialise and play. However, these technologies also present challenges and risks. Online safety is therefore an essential element of safeguarding students and protecting them from harm in the digital world. Students must be supported to be able to learn how to develop strategies to manage and respond to risk so they can be empowered to build resilience online.

Poole Grammar School has a duty to provide the school community with quality internet access to raise educational standards, promote student achievement, support the professional work of staff and enhance the school's management functions. The use of online services is embedded throughout PGS, and so there must be controls in place to keep students safe.

The school Online Safety Policy:

- sets expectations for the safe and responsible use of digital technologies for learning, administration, and communication
- allocates responsibilities for the delivery of the policy
- is regularly reviewed in a collaborative manner, taking account of online safety incidents and changes/trends in technology and related behaviours
- establishes guidance for staff in how they should use digital technologies responsibly, protecting themselves and the school and how they should use this understanding to help safeguard students in the digital world
- describes how the school will help prepare students to be safe and responsible users of online technologies
- establishes clear procedures to identify, report, respond to and record the misuse of digital technologies and online safety incidents, including external support mechanisms
- is supplemented by a series of related acceptable use agreements
- is made available to staff at induction and through MyConcern
- is published on the school website.

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

- Content: being exposed to illegal, inappropriate or harmful content, for example: pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism.
- Contact: being subjected to harmful online interaction with other users; for example: peer to peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes.
- Conduct: personal online behaviour that increases the likelihood of, or causes, harm; for example, making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography, sharing other explicit images and online bullying).
- Commerce: risks such as online gambling, inappropriate advertising, phishing and or financial scams.



## 2. Scope of the Online Safety Policy

This Online Safety Policy outlines the commitment of Poole Grammar School 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 and technology, both in and out of the school. It also applies to the use of personal digital technology on the school site (where permitted).**

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

This policy must be read in conjunction with other relevant PGS policies including (but not limited to) Safeguarding, Anti-bullying, Behaviour, Taking Using And Storing Images Of Students, confidentiality, screening, searching and relevant curriculum policies including computing, Relationships and Sex Education (RSE) Policy and Staff Code of Conduct.

The PGS Online Safety Lead is currently Nathan Chase, Deputy Designated Safeguarding Lead.

## 3. Policy development, monitoring and review

This Online Safety Policy has been developed by the Online Safety Lead in consultation with Senior Leaders and staff.

The governing body, headteacher, SLT and Online Safety Lead review this policy in full on an annual basis and following any online safety incidents. The next scheduled review date for this policy is July 2024.

The school will monitor the impact of the policy using:

- logs of reported incidents
- monitoring logs of internet activity (including sites visited)
- internal monitoring data for network activity

This policy has due regard to all relevant legislation and guidance including, but not limited to, the following:

- [Voyeurism \(Offences\) Act 2019](#)
- [The UK General Data Protection Regulation \(UK GDPR\)](#)
- [Data Protection Act 2018](#)
- [DfE \(2021\) 'Harmful online challenges and online hoaxes'](#)
- [DfE \(2023\) 'Keeping children safe in education 2023'](#)
- [Department for Digital, Culture, Media and Sport and UK Council for Internet Safety \(2020\) 'Sharing nudes and semi-nudes: advice for education settings working with children and young people'](#)
- [DfE \(2023\) 'Teaching online safety in school'](#)
- [DfE \(2022\) 'Searching, screening and confiscation'](#)
- [National Cyber Security Centre \(2018\) 'Small Business Guide: Cyber Security'](#)
- [UK Council for Child Internet Safety \(2020\) 'Education for a Connected World – 2020 edition'](#)
- [DfE \(2022\) 'Meeting Digital and Technology Standards in Schools & Colleges'](#)
- [UKCIS \(2020\) 'Sharing nudes and semi-nudes: advice for education settings working with children and young people'](#)



## 4. Roles & Responsibilities

The governing board is responsible for:

- Ensuring that this policy is effective and complies with relevant laws and statutory guidance.
- Ensuring the Safeguarding teams remit covers online safety.
- Reviewing this policy on an annual basis.
- Ensuring their own knowledge of online safety issues is up to date by undertaking training.
- Ensuring all staff undergo safeguarding and child protection training, including online safety, at induction.
- Ensuring that there are appropriate filtering and monitoring systems in place and that leadership teams and relevant staff have an awareness of the provisions in place, manage them effectively and know how to escalate concerns when identified.
- Ensuring that all relevant school policies have an effective approach to planning for, and responding to, online challenges and hoaxes embedded within them.

The headteacher is responsible for:

- Ensuring that online safety is a running and interrelated theme throughout the school's policies and procedures, including in those related to the curriculum, teacher training and safeguarding.
- Supporting the Online Safety Lead by ensuring they have enough time and resources to carry out their responsibilities in relation to online safety.
- Ensuring staff receive regular, up-to-date and appropriate online safety training and information as part of their induction and safeguarding training.
- Ensuring online safety practices are audited and evaluated.
- Supporting staff to ensure that online safety is embedded throughout the curriculum so that all students can develop an appropriate understanding of online safety.
- As part of the shortlisting process, consider carrying out an online search as part of their due diligence on shortlisted candidates to help identify any incidents or issues that have happened, and are publicly available online which the school/ academy might want to explore with applicants at interview.
- Working with the DSL and governing board to update this policy on an annual basis.

The Designated Safeguarding Lead (DSL) is responsible for:

- Holding the lead responsibility for online safety, within their safeguarding role.
- Ensuring they receive relevant and regularly updated training in online safety to enable them to understand the risks associated with online safety and be confident that they have the relevant knowledge and up to date capability required to keep children safe whilst they are online
- Meeting regularly with the Safeguarding Governor and Online Safety Lead to discuss current issues, review (anonymised) incidents and filtering and monitoring logs and ensuring that annual (at least) filtering and monitoring checks are carried out
- liaise with staff and IT providers on matters of safety and safeguarding and welfare (including online and digital safety)

The Online Safety Lead (OSL) is responsible for:

- Acting as the named point of contact within the school on all online safeguarding issues.
- Undertaking training so they understand the risks associated with online safety and can recognise additional risks that students with SEND face online.
- Liaising with relevant members of staff on online safety matters, e.g. the SENDCO and the Network team.
- Ensuring online safety is promoted to parents/carers and the wider community through a variety of channels and approaches.
- Ensuring safeguarding is considered in the school's approach to remote learning.



- Receiving reports of online safety incidents and handling them.
- Ensuring appropriate referrals are made to external agencies, as required.
- Working closely with the police during police investigations.
- Accessing regular and appropriate training and support to ensure they understand the unique risks associated with online safety and have the relevant up to date knowledge to keep students safe online.
- Coordinating the school's participation in local and national online safety events, e.g. Safer Internet Day.
- Establishing a procedure for reporting online safety incidents and inappropriate internet use, both by students and staff.
- Ensuring all members of the school community understand the reporting procedure.
- Maintaining records of reported online safety concerns as well as the actions taken in response to concerns.
- Monitoring online safety incidents to identify trends and any gaps in the school's provision and using this data to update the school's policies and procedures.
- Reporting online safety concerns as appropriate to the SLT and to the governing board
- Updating and reviewing this policy on a regular basis (at least annually).

The Head of Life Skills/PSHE is responsible for:

- Ensuring that matters of online safety education are covered as part of the Life Skills/PSHE curriculum in an age appropriate way

The Network Team are responsible for:

- Providing the technical support and perspective to the DSL, Online Safety Lead and Senior Leadership Team, especially in the development and implementation of appropriate online safety policies and procedures.
- Implementing appropriate security measures as directed by the SLT, to ensure that the IT systems are secure and not open to misuse or malicious attack, whilst allowing learning opportunities to be maximised.
- Ensuring the school meets (as a minimum) the required online safety technical requirements as identified by the DfE Meeting Digital and Technology Standards in Schools & Colleges.
- Ensuring that our filtering policy is applied and updated on a regular basis. The responsibility for its implementation is shared with the Online Safety Lead.
- Ensuring that our monitoring systems are applied and updated on a regular basis. The responsibility for its implementation is shared with the Online Safety Lead.
- Ensuring that appropriate access and technical support is given to the Online Safety Lead to our filtering and monitoring systems, to enable him/her to take appropriate safeguarding action if/when required.

All staff members are responsible for:

- Contributing to the development of online safety policies.
- Taking responsibility for the security of ICT systems and electronic data they use or have access to.
- To read PGS's Acceptable Use Agreement and adhere to it.
- Modelling good online behaviours.
- Maintaining a professional level of conduct in their personal use of technology, both on and off site.
- Having an awareness of online safety issues, and how they relate to the students in their care, including understanding the key issues related to online safety; content, contact, conduct and commerce.
- Ensuring they are familiar with, and understand, the indicators that students may be unsafe online.
- Reporting concerns in line with the school's reporting procedure.



- Where relevant to their subject, ensuring online safety is embedded in their teaching of the curriculum.
- Ensuring that when supervising computer or device use, students use is actively monitored.
- Knowing when and how to escalate online safety issues, internally and externally.
- Taking personal responsibility for professional development in this area.

Students are responsible for:

- Reading PGS's Acceptable Use Agreement and adhering to it.
- Respecting the feelings and rights of others both on and offline.
- Seeking help from a member of staff if things go wrong or they are concerned about something they or a peer have experienced online.
- Taking responsibility for keeping themselves and others safe online.
- Assessing the personal risks of using any particular technology and behave safely and responsibly to limit those risks.
- Reporting online safety incidents and concerns in line with the procedures within this policy.

All parents/carers are responsible for:

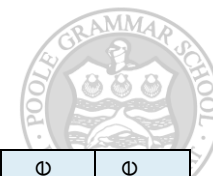
- Reading PGS's Acceptable Use Agreement, encouraging their child to adhere to it, and adhering to it themselves where appropriate.
- Supporting PGS's online safety approaches by discussing online safety issues with their children and reinforcing appropriate and safe online behaviours at home.
- To role model safe and appropriate uses of new and emerging technology.
- Seeking help and support from PGS, or other appropriate agencies, if they or their child encounters online problems or concerns.
- Contributing to the development of PGS's online safety policy.
- Using PGS's systems, and other network resources, safely and appropriately.
- Reporting any known issues as soon as possible.

## 5. 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:

- Student planners
- Staff induction and code of conduct
- Splash screens
- Posters/notices around where technology is used
- Communication with parents/carers
- Built into education sessions
- School website
- Peer support



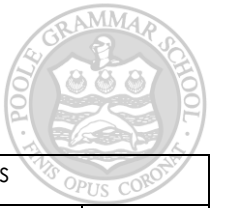
User actions		Acceptable	Acceptable at certain times	Acceptable for nominated	Unacceptable	Unacceptable and illegal
Users shall not access online content (including apps, games, sites) to make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	<p><b>Any illegal activity for example:</b></p> <ul style="list-style-type: none"> <li>• Child sexual abuse imagery*</li> <li>• Child sexual abuse/exploitation/grooming</li> <li>• Terrorism</li> <li>• Encouraging or assisting suicide</li> <li>• Offences relating to sexual images i.e., revenge and extreme pornography</li> <li>• Incitement to and threats of violence</li> <li>• Hate crime</li> <li>• Public order offences - harassment and stalking</li> <li>• Drug-related offences</li> <li>• Weapons / firearms offences</li> <li>• Fraud and financial crime including money laundering</li> </ul>					X
Users shall not undertake activities that might be classed as cyber-crime under the Computer Misuse Act (1990)	<ul style="list-style-type: none"> <li>• 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)</li> <li>• Gaining unauthorised access to school networks, data and files, through the use of computers/devices</li> <li>• Creating or propagating computer viruses or other harmful files</li> <li>• Revealing or publicising confidential or proprietary information (e.g., financial / personal information, databases, computer / network access codes and passwords)</li> <li>• Disable/Impair/Disrupt network functionality through the use of computers/devices</li> <li>• Using penetration testing equipment (without relevant permission)</li> </ul>					X
Users shall not undertake activities that are not illegal but are classed as	Accessing inappropriate material/activities online in a school setting including pornography, gambling, drugs. (Informed by the school's filtering practices and/or AUAs)			X	X	
	Promotion of any kind of discrimination				X	
	Using school systems to run a private business				X	



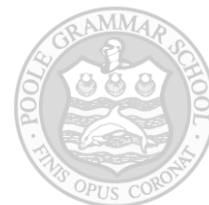


User actions		Acceptable	Acceptable at certain times	Acceptable for nominated	Unacceptable	Unacceptable and illegal
unacceptable in school policies:	Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school				X	
	Infringing copyright				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	

When the following activities are undertaken for non-educational purposes:	Staff and other adults				Students			
	Not allowed	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission/awareness
Online gaming	X				X			
Online shopping/commerce	X				X			
File sharing	X				X			
Social media	X				X			
Messaging/chat	X				X			



When the following activities are undertaken for non-educational purposes:	Staff and other adults				Students			
	Not allowed	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission/awareness
Entertainment streaming e.g. Netflix, Disney+	X				X			
Use of video broadcasting, e.g. YouTube, Twitch, TikTok	X				X			
Mobile phones may be brought to school		X				X		
Use of mobile phones for learning at school		X			X			
Use of mobile phones in social time at school		X			X			
Taking photos on mobile phones/cameras	X				X			
Use of other personal devices, e.g. tablets, gaming devices		X			X			
Use of personal e-mail in school, or on school network/wi-fi			X				X	
Use of school e-mail for personal e-mails	X					X		




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

## 6. Reporting and Responding

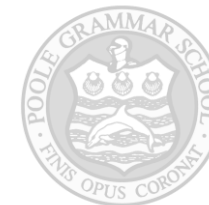
The school will take all reasonable precautions to ensure online safety for all school users but recognises that incidents may occur inside and outside of the school (with impact on the school) which will need intervention. The school will ensure:

- 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 (see flowchart on the following pages), 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
- incidents should be referred to the Online Safety Lead and this should ordinarily be done by completing the Online Safety Incident Report form, as in Appendix 3.3 of this policy.
- incidents regarding online safety will be logged by the Online Safety Lead using the log form as in Appendix 3.4 or a suitable alternative and will be stored by the Online Safety Lead. It will contain as a minimum information regarding students affected, the nature of the incident, actions taken as a result of the incident.
- Incidents can also be raised in other ways but attention is drawn to the required details as in appendix 3.3:
  - All members of the community:
    - the anonymous online form via Whisper ([Whisper Anonymous Reporting | SWGfL](#))
    - the reporting software NetSupport DNA, accessible from the system tray on the taskbar, available on all school computers 
    - by talking to/emailing the online safety lead (Mr Chase; [chasen@poolegrammar.com](mailto:chasen@poolegrammar.com) )
    - by talking to/emailing one of the safeguarding team ([pgsafeguarding@poolegrammar.com](mailto:pgsafeguarding@poolegrammar.com) )
  - by Staff related to students:
    - using MyConcern ([myconcern.education](http://myconcern.education))

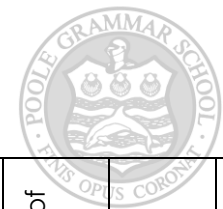
- by Students:
  - by informing a member of staff who should then refer it to the safeguarding team
- Where one of these alternative methods of informing the Online Safety Lead of an incident are used, the Online Safety Incident Record form (Appendix 3.4) will be completed by the Online Safety Lead in lieu of the report form.
- relevant logs will also be completed on MyConcern as appropriate.
- where there is no suspected illegal activity, devices may be checked using the following procedures (the log as in appendix 3 should be completed):
  - at least two members of staff should be involved, which should include the Online Safety Lead, or if unavailable, the DSL or a deputy DSL
  - conduct the procedure using a designated device that will not be used by students 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 (as relevant)
    - police involvement and/or action
- there are support strategies in place e.g., peer support for those reporting or affected by an online safety incident
- relevant staff are aware of external sources of support and guidance in dealing with online safety issues, e.g. local authority; police; Professionals Online Safety Helpline; Reporting Harmful Content; CEOP.
- those involved in the incident will be provided with feedback about the outcome of the investigation and follow up actions (as relevant)
- learning from the incident (or pattern of incidents) will be provided (as relevant and anonymously) to:
  - 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

It is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the school community are aware that incidents have been dealt with.

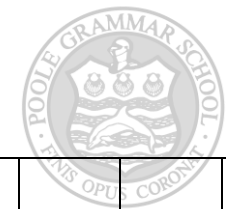
The tables on the following page gives guidance as to how certain types of incident related to computer, device and system use should be dealt with. It is intended that incidents of misuse of computer facilities will be dealt with through normal behaviour/disciplinary procedures and therefore be referred to heads of year for investigation and follow up, but incidents with an element of online safety risk be referred initially to the Online Safety Lead.



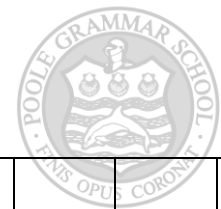
Incidents – Responding to Student Actions – Misuse of systems	Issue a warning	Record details on SIMS	Issue sanction in line with behaviour management policy	Record on MyConcern	Refer to Head of Year	Refer to SLT	Refer to Online Safety Lead/DSL	Inform network team – filtering or other technical actions required	Inform network team – removal of device/network/internet access rights	Refer to Police/Social Work	Explicitly Inform parents/carers (not just via SIMS)
Attempting to access or accessing the school network, using another user's account (staff or learner) or allowing others to access school network by sharing username and passwords		X	X					X	X		
Corrupting or destroying the data of other users.		X	X		X			X	X		
Unauthorised downloading or uploading of files or use of file sharing.		X	X					X	X		
Unauthorised use of digital devices (including taking images)		X			X	X					X
Continued infringements of the above, following previous warnings or sanctions.		X				X	X		X	(X)	X



Incidents – Responding to Student Actions – Misuse with an online safety risk	Issue a warning	Record details on SIMS	Issue sanction in line with behaviour management policy	Record on MyConcern	Refer to Head of Year	Refer to SLT	Refer to Online Safety Lead/DSL	Inform network team – filtering or other technical actions required	Inform network team – removal of device/network/internet access rights	Refer to Police/Social Work	Explicitly Inform parents/carers (not just via SIMS)
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable/inappropriate activities).		X		X			X	X	X	(X)	X
Sending an e-mail, text or message that is regarded as offensive, harassment or of a bullying nature		X	X				X				
Using proxy sites or other means to subvert the school's filtering system.		X		X			X	X	X		X
Accidentally accessing offensive or pornographic material and <b>reporting</b> the incident.							X	X			
Accidentally accessing offensive or pornographic material and <b>failing</b> to report the incident.		X	X				X	X			
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act.		X					X		X		
Unauthorised use of online services		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
Continued infringements of the above, following previous warnings or sanctions.		X					X		X	(X)	X



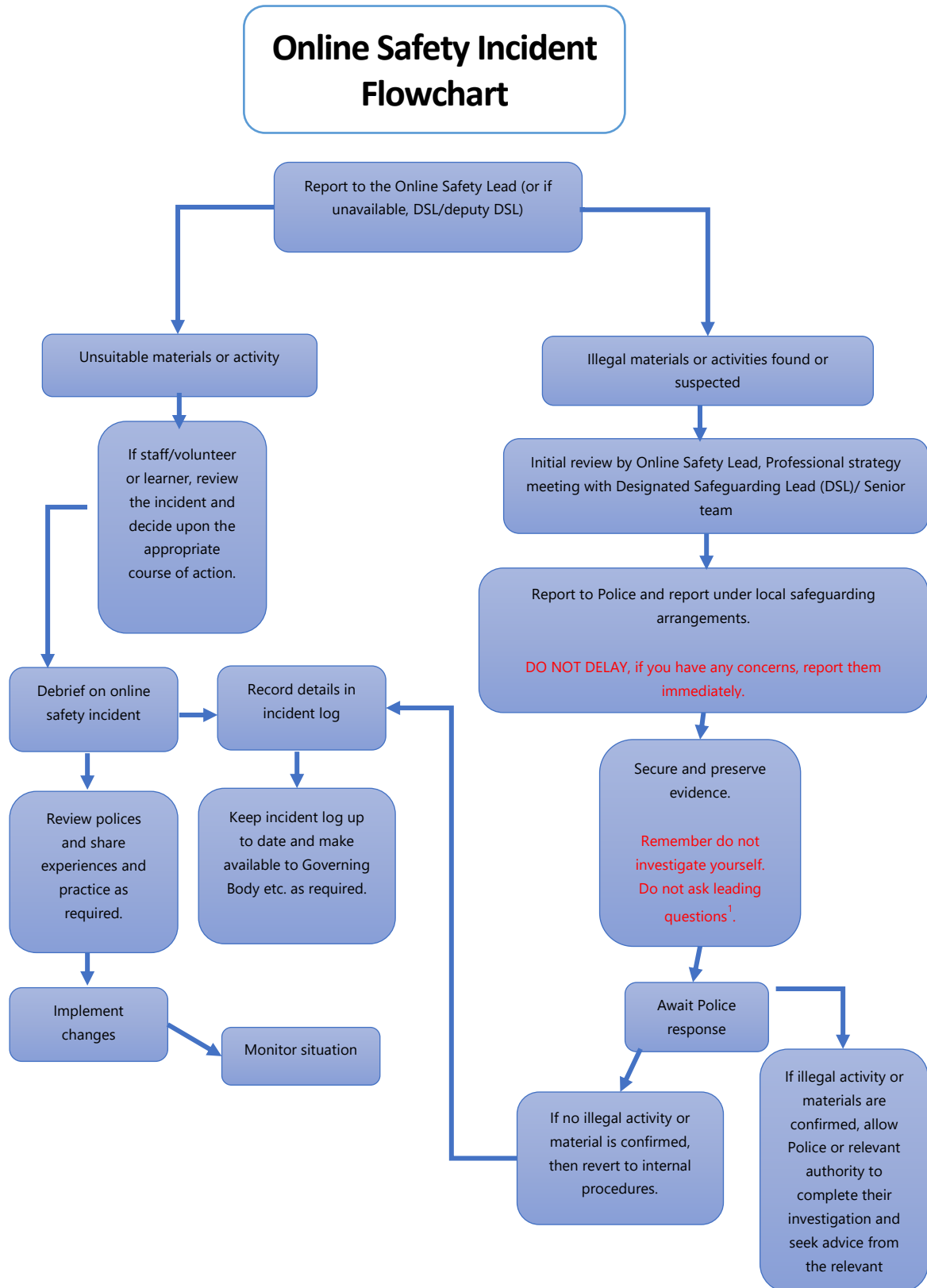
Incidents – Responding to Staff Actions	Refer to line manager	Refer to Headteacher	Refer to HR	Refer to Police	Refer to Network Team for action re filtering, etc.	Issue a warning	Suspension	Disciplinary action
Deliberately accessing or trying to access material that could be considered illegal (see list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



Incidents – Responding to Staff Actions	Refer to line manager	Refer to Headteacher	Refer to HR	Refer to Police	Refer to Network Team for action re filtering, etc.	Issue a warning	Suspension	Disciplinary action
Inappropriate personal use of the digital technologies e.g. social media / personal e-mail	X		X			X	X	
Careless use of personal data, e.g. displaying, holding or transferring data in an insecure manner	X		X			X	X	
Actions which could compromise the staff member's professional standing		X	X				X	X
Actions which could bring the school into disrepute or breach the integrity or the ethos of the school.		X	X			X	X	X
Failing to report incidents whether caused by deliberate or accidental actions		X	X			X	X	X
Continued infringements of the above, following previous warnings or sanctions.		X	X				X	X



Incidents with an element of online safety risk should be referred initially to the Online Safety Lead. The following flowchart indicates the decision-making path where such incidents are referred to the Online Safety Lead/DSL:





## 7. Online Safety Education Programme

We will establish and embed a progressive online safety curriculum to raise awareness and promote safe and responsible use of technology among students by:

- Ensuring education regarding safe and responsible use precedes Internet access
- Including online safety in Life Skills/PSHE and computing programmes of study
- Reinforcing online safety messages whenever technology or the Internet is in use
- Educating students in the effective use of the Internet to research; including the skills of knowledge location, retrieval and evaluation
- Teaching students to be critically aware of the materials they read and shown how to validate information before accepting its accuracy

We will support students to read and understand the acceptable use policies in a way which suits their age and ability by:

- Displaying acceptable use posters in all rooms with Internet access
- Informing students that network and Internet use will be monitored for safety and security purposes and in accordance with legislation
- Seeking student voice when writing and developing online safety policies and practices, including curriculum development and implementation
- Using support, such as external visitors, where appropriate, to complement and support our internal online safety education approaches

## 8. Education and Engagement of Staff/Volunteers

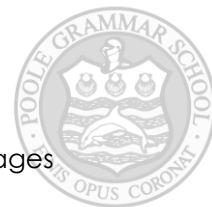
All staff will receive online safety training and understand their responsibilities as outlined in this policy. This will include the following:

- The online safety (e-safety) policy will be formally provided to and discussed with all members of staff as part of induction and will be reinforced and highlighted as part of PGS safeguarding practice on an annual basis; staff will be asked to sign off that they have read the policy using MyConcern.
- To protect staff and students, PGS implements an Acceptable Use Agreement which highlights appropriate online conduct and communication.
- Staff will be made aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.
- Up-to-date and appropriate staff training in safe and responsible Internet use, both professionally and personally, will be provided for all members of staff on a regular basis.
- Staff with a responsibility for managing filtering systems or monitor ICT use will be supervised by the Senior Leadership Team and will have clear procedures for reporting issues or concerns.
- PGS will highlight useful online tools which staff should use with students in the classroom. These tools will vary according to the age and ability of the students.
- Staff will be made aware that their online conduct out of PGS could have an impact on their role and reputation within PGS. Civil, legal or disciplinary action could be taken if they are found to bring the profession or institution into disrepute, or if something is felt to have undermined confidence in their professional abilities.
- The Online Safety Lead and Designated Safeguarding Lead will receive regular updates through attendance at external training events, (e.g. UKSIC / SWGfL / other relevant organisations) and by reviewing guidance documents released by relevant organisations
- The Online Safety Lead will provide advice/guidance/training to individuals as required.

## 9. Education and Engagement of Parents/Carers

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

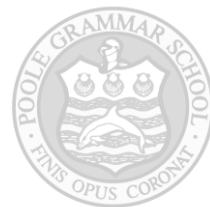


- the students – who are encouraged to pass on to parents the online safety messages they have learned in lessons
- letters, newsletters, website, learning platform
- high profile events / campaigns e.g. Safer Internet Day
- reference to the relevant web sites/publications, e.g. SWGfL; [www.saferinternet.org.uk](http://www.saferinternet.org.uk) ; [www.childnet.com/parents-and-carers](http://www.childnet.com/parents-and-carers)

## 10. Technology

### 10.1 Filtering

- The school manages access to content across its systems for all users using the schools internet provision. The filtering provided meets the standards defined in the DfE Filtering standards for school and colleges UK Safer Internet Centre Appropriate filtering.
- Access to online content and services is managed for all users
- Illegal content (e.g., child sexual abuse images) is filtered by the 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 by the service providers
- Filtering policies are agreed by senior leaders and technical staff in line with informed risk assessment, and are regularly reviewed and updated in response to changes in technology and patterns of online safety incidents/behaviours.
- Changes to the filtering policies will be risk assessed by staff with educational and technical experience and, where appropriate, with consent from the Senior Leadership Team.
- The Online Safety Lead will ensure that regular checks (at least once a year) are carried out to ensure that filtering methods are effective and appropriate. This will be via the SWGfL tool found here: <http://testfiltering.com/> . Results of the tests will be shared with SLT and logged as part of the minutes of SLT meetings.
- School computers:
  - The RM SafetyNet proxy filtering service is used for all members of the school community using a school computer.
  - All internet access is logged against a particular computer, and can be traced to the user logged on at the time.
  - Logs are maintained for 1 year.
  - Staff have access to a service which bypasses the RM SafetyNet filtering service.
    - Staff are issued with individual usernames and passwords for this service.
    - Any internet access through this service is logged against the staff member.
    - This service is filtered using the IWF filtering.
  - RM SafetyNet logs are checked when issues are raised to see which users have been affected.
  - During lessons, NetSupport Tutor adds a further level of internet filtering if enabled by the member of staff supervising the class.
- “Bring Your Own Devices”
  - Staff and students can connect permitted wi-fi devices to the PGSBYOD wi-fi network.
  - All users of the PGSBYOD wi-fi network must log in using their school network credentials.
  - Smoothwall proxy filtering service is used for Internet access via this wi-fi network.
  - All internet access via this service is logged against the user.
  - Logs are maintained for 90 days.
  - This network provides filtered access to the internet, blocking according to the Internet Watch Foundation CAIC list and also Adult Content.
  - Internet access is logged against the device accessing the service.
  - Only the headteacher, certain members of the SLT and network manager are informed of the password for access to this service.
- there are established and effective routes for users to report inappropriate content
  - Any reports should be made using one of the following available systems or methods:



- All:
  - the anonymous online form via Whisper (Whisper Anonymous Reporting | SWGfL)
  - the reporting software NetSupport DNA, accessible from the system tray on the taskbar, available on all school computers
  - by talking to/emailing the online safety lead (Mr Chase; chasen@poolegrammar.com)
  - by talking to/emailing one of the safeguarding team (pgssafeguarding@poolegrammar.com)
  - Using the forms as found in Appendix 3.
- by Staff related to students:
  - using MyConcern (myconcern.education)
- by Students:
  - by informing a member of staff who should then refer it to the Online Safety team
- Where one of these alternative methods of informing the Online Safety Lead of an incident are used, the Online Safety Incident Record form (Appendix 3.4) will be completed by the Online Safety Lead in lieu of the report form.
- there is a clear process in place to deal with requests for filtering changes.
  - Requests by staff to remove a block or add a block can be made by using the "filtering change request form" found in Appendix 3.2 and should be submitted to the Online Safety Lead for consideration.
  - Any requests received will be considered by at least two senior staff to include either the Online Safety Lead or in their absence the DSL.

## 10.2 Monitoring

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

- The school monitors all network use across all its devices and services using NetSupport DNA.
- Logs created by Netsupport DNA are kept for at least 1 month.
- The school monitors all internet use via RM Safetynet or Smoothwall depending on method of access.
- An appropriate monitoring strategy for all users has been agreed and users are aware that the network is 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 and referred to the Online Safety Lead as appropriate.

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

- physical monitoring:
  - during lessons: adult supervision in the classroom; main computer rooms (CR1-CR5) are set up so that the screen faces the teacher's desk
  - during lunchtime: supervision by 6th form computer monitors
  - in the library: by library staff who regularly check students using the computers
  - where not in use, computer rooms should be locked
- NetSupport Tutor is installed on the teacher computers in all computer rooms. It allows the monitoring of computer screens in computer rooms by the teacher from their computer. It can be used to view screens, take control of computers and monitor and restrict internet access
- NetSupport DNA provides keyword and phrase monitoring - Using a database of over 14,000 pre-supplied safeguarding keywords and phrases covering a range of topics from self-harm, bullying and racism, through to risks of radicalisation and child



exploitation, NetSupport DNA monitors for students triggering these terms in the text being typed, copied or searched for.

- NetSupport DNA logs are checked regularly by the network team and any breaches or events of concern are flagged to the Online Safety Lead
- pro-active alerts inform the school of breaches to the filtering policy, allowing effective intervention.
- Internet use is logged, regularly monitored and reviewed.

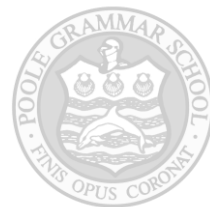
### 10.3 Technical Security

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

- responsibility for technical security resides with SLT who may delegate activities to identified roles.
- all users have clearly defined access rights to school technical systems and devices.
- password policy and procedures are implemented.
- the security of their username and password and must not allow other users to access the systems using their log on details.
- all users have responsibility for the security of their username and password and must not allow other users to access the systems using their log on details.
- all school networks and system will be protected by secure passwords. Passwords must not be shared with anyone.
- the administrator passwords for school systems are kept in a secure place.
- there is a risk-based approach to the allocation of learner usernames and passwords.
- there will be regular reviews and audits of the safety and security of school technical systems.
- servers, wireless systems and cabling are securely located and physical access restricted.
- appropriate security measures are in place (schools may wish to provide more detail which may need to be provided by the service provider) to protect the servers, firewalls, routers, wireless systems and devices from accidental or malicious attempts which might threaten the security of the school systems and data. These are tested regularly. The school infrastructure and individual workstations are protected by up-to-date endpoint software.
- there are rigorous and verified back-up routines, including the keeping of network-separated (air-gapped) copies off-site or in the cloud.
- The Network Manager is responsible for ensuring that all software purchased by and used by the school is adequately licenced and that the latest software updates (patches) are applied.
- use of school devices out of school and by family members is regulated by an acceptable use statement that a user consents to when the device is allocated to them
- personal use of any device on the school network is regulated by acceptable use statements that a user consents to when using the network
- staff members are not permitted to install software on a school-owned devices without the consent of the SLT/Network Manager
- removable media is not permitted unless approved by the SLT/Network Manager
- systems are in place to control and protect personal data and data is encrypted at rest and in transit. (See school personal data policy template in the appendix for further detail)
- mobile device security and management procedures are in place (where mobile devices are allowed access to school systems).
- guest users are provided with appropriate access to school systems based on an identified risk profile.

The school technical systems will be managed in ways that ensure that the school meets recommended technical requirements. Further details can be located in the following policies:

- Information Security Policy
- Password Security Policy



## 10.4 Mobile technologies

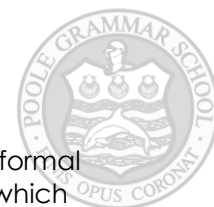
The widespread ownership of mobile phones and a range of other personal devices, including wearable technologies, among children, young people and adults will require all members of the PGS community to take steps to ensure that mobile phones and personal devices are used responsibly.

### 10.4.1 Expectations for safe use of personal devices and mobile phones

- Electronic devices of all kinds that are brought into PGS are the responsibility of the user at all times. PGS accepts no responsibility for the loss, theft or damage of such items. Nor will PGS accept responsibility for any adverse health effects caused by any such devices either potential or actual.
- The sending of abusive or inappropriate messages or content via mobile phones or personal devices is forbidden by any member of the PGS community and any breaches will be dealt with as part of the PGS discipline/behaviour policy.
- Members of staff will be issued with an email address where contact with students or parents/carers is required.
- All members of the PGS community will be advised to take steps to protect their mobile phones or devices from loss, theft or damage.
- All members of the PGS community will be advised to use passwords/pin numbers to ensure that unauthorised calls or actions cannot be made on their phones or devices if they are lost or stolen. Passwords and pin numbers should be kept confidential. Mobile phones and personal devices should not be shared.
- All members of the PGS community will be advised to ensure that their mobile phones and personal devices do not contain any content which may be considered to be offensive, derogatory or would otherwise contravene PGS's policies.
- PGS mobile phones and devices must always be used in accordance with the AUA
- PGS mobile phones and devices used for communication with parents and students must be suitably protected via a passcode/password/pin and must only be accessed and used by members of staff.

### 10.4.2 Students use of personal devices and mobile phones

- Students will be instructed in safe and appropriate use of mobile phones and personal devices and will be made aware of boundaries and consequences.
- For main school students, mobile phones will be switched off and kept in bags or lockers, out of sight, throughout the day. They must not be seen or used between arrival on the school site and leaving the school site. The only exception is for students who need to access their electronic bus pass at the end of the day.
- For sixth form students, mobile phones will be switched off and kept in bags or lockers, out of sight, during lessons. They may only be used by sixth form students in the sixth form quiet study area and the library, and only for educational purposes. The use of mobile phones or any devices to make phone calls, play games or access the internet for any purpose other than educational pursuits is strictly forbidden.
- Where a student has a clear medical requirement to use their mobile phone or device (e.g. to monitor blood sugar levels) they will be permitted to do so under strict conditions and agreement regarding the locations in which the devices can be used. If the student is found to be using their mobile phone or device for any other reason, then they should expect that their device will be confiscated in line with the schools behaviour/discipline policy.
- Exceptions will be made to these rules where a student with SEND has a specific requirement (such as accessibility features).
- Where special exceptions are required, these will be agreed by the Deputy Head with responsibility for SEND and information communicated to all staff.
- Headphones and earphones may not be used by any student, except for sixth form students in the sixth form quiet study area for educational purposes such as watching online lectures or educational films.



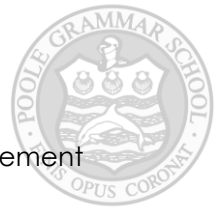
- Mobile phones or personal devices will not be used by students during lessons or formal PGS time unless as part of an approved and directed curriculum-based activity which has consent from the Senior Leadership Team. The use of personal mobile phones or devices for a specific education purpose does not mean that blanket use is permitted.
- If members of staff have an educational reason to allow students to use their mobile phones or personal devices as part of an educational activity then it will only take place once approved by the Senior Leadership Team.
- If a student needs to contact their parents/carers they will be allowed to use a PGS phone. Parents are advised not to contact their child via their mobile phone during the school day, but to contact the PGS office. Exceptions may be permitted in exceptional circumstances on a case-by-case basis and as approved by the headteacher.
- Students should protect their phone numbers by only giving them to trusted friends and family members.
- Phones and devices must not be taken into examinations.
- Students found in possession of a mobile phone or personal device during an exam will be reported to the appropriate examining body. This may result in the student's withdrawal from either that examination or all examinations.

If a student breaches the policy, the phone or device will be confiscated and will be held in a secure place in line with the schools behaviour/discipline policy.

- Staff may confiscate a student's mobile phone or device if they believe it is being used to contravene our behaviour or bullying policy or could contain youth produced sexual imagery (sexting).
- Searches of mobile phone or personal devices will only be carried out in accordance with our policy. ([www.gov.uk/government/publications/searching-screening-and-confiscation](http://www.gov.uk/government/publications/searching-screening-and-confiscation))
- Students' mobile phones or devices may be searched by a member of the Senior Leadership team, with the consent of the student or a parent/ carer. Content may be deleted or requested to be deleted, if it contravenes our policies. ([www.gov.uk/government/publications/searching-screening-and-confiscation](http://www.gov.uk/government/publications/searching-screening-and-confiscation))
- If there is suspicion that material on a student's personal device or mobile phone may be illegal or may provide evidence relating to a criminal offence, the device will be handed over to the police for further investigation.

#### 10.4.3 Staff use of personal devices and mobile phones

- Members of staff are not permitted to use their own personal phones or devices for contacting students, young people and their families within or outside of PGS in a professional capacity. Any pre-existing relationships which could compromise this must be discussed with a senior leader.
- Staff will not use personal devices such as mobile phones, tablets or cameras to take photos or videos of students and will only use work-provided equipment for this purpose.
- Staff will not use any personal devices directly with students and will only use work-provided equipment during lessons/educational activities.
- Staff personal mobile phones and devices will be switched off/switched to 'silent' mode during lesson times.
- Bluetooth or other forms of communication should be "hidden" or switched off during lesson times.
- Personal mobile phones or devices will not be used during teaching periods unless permission has been given by a member of Senior Leadership Team. The only exception to this rule is if mobile phones or devices are required for two factor authentication systems that may be in place for school systems.
- Staff will ensure that any content bought on site via mobile phones and personal devices are compatible with their professional role and expectations.
- If a member of staff breaches PGS policy then disciplinary action will be taken.
- If a member of staff is thought to have illegal content saved or stored on a mobile phone or personal device or have committed a criminal offence then the police will be



contacted and allegations will be responded to following the allegations management policy.

#### 10.4.4 Visitors use of personal devices and mobile phones

- Parents/carers and visitors must use mobile phones and personal devices in accordance with PGS's policy.
- Use of mobile phones or personal devices by visitors and parents/carers to take photos or videos must take place in accordance with PGS's Image Use policy.
- Staff will be expected to challenge concerns when safe and appropriate and will always inform the DSL of any breaches of use by visitors.

### 10.5 Social Media

Expectations regarding safe and responsible use of social media will apply to all members of the PGS community and exist in order to safeguard both the school and the wider community, on and offline. Examples of social media may include blogs, wikis, social networking, forums, bulletin boards, multiplayer online gaming, apps, video/photo sharing sites, chatrooms, instant messenger and many others.

- All members of the PGS community will be encouraged to engage in social media in a positive, safe and responsible manner at all times.
- Information about safe and responsible use of social media will be communicated clearly and regularly to all members of the PGS community.
- All members of the PGS community are advised not to publish specific and detailed private thoughts, concerns, pictures or messages on any social media services, especially content that may be considered threatening, hurtful or defamatory to others.
- PGS will control students and staff access to social media and social networking sites whilst on site and using PGS provided devices and systems.
- The use of social networking applications during PGS hours for personal use is not permitted.
- Inappropriate or excessive use of social media during PGS hours or whilst using PGS devices may result in disciplinary or legal action and/or removal of Internet facilities.

Any concerns regarding the online conduct of any member of the PGS community on social media sites should be reported to the Senior Leadership Team and will be managed in accordance with existing PGS policies such as anti-bullying, allegations against staff, behaviour and safeguarding/child protection.

Any breaches of PGS policy may result in criminal, disciplinary or civil action being taken and this will depend upon the age of those involved and the circumstances of the wrong committed.

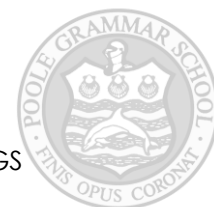
Action taken will be in accordance with the relevant PGS policies, such as anti-bullying, allegations against staff, behaviour and safeguarding/child protection.

#### 10.5.1 Official use of social media

The school has several official social media channels that are only used for educational or engagement purposes. Staff members must be authorised by the headteacher to access the school's social media accounts.

- Official use of social media sites by PGS will only take place with clear educational or community engagement objectives with specific intended outcomes e.g. increasing parental engagement.
- Official use of social media sites as communication tools will be risk assessed and formally approved by the headteacher.
- Official PGS social media channels will be set up as distinct and dedicated social media site or account for educational or engagement purposes.





- Staff will use PGS provided email addresses to register for and manage official PGS approved social media channels.
- Staff running official PGS social media channels will ensure that they are aware of the required behaviours and expectations of use. They will ensure that sites are used safely, responsibly and in accordance with local and national guidance and legislation.
- All communication on official PGS social media platforms will be clear, transparent and open to scrutiny.
- Any online publication on official PGS social media sites will comply with legal requirements and will not breach any common law duty of confidentiality, copyright etc.
- Official social media use by PGS will be in line with existing policies, including: anti-bullying and child protection.
- Images or videos of students will only be shared on official PGS social media sites/channels in accordance with PGS's Taking Using And Storing Images Of Students policy.
- Information about safe and responsible use of PGS social media channels will be communicated clearly and regularly to all members of the PGS community.
- Official social media sites, blogs or wikis and associated accounts will be suitably protected (e.g. password protected) and where possible/appropriate, run and/or linked to from the PGS website and take place with written approval from Senior Leadership Team.
- Senior Leadership Team staff must be aware of account information and relevant details for social media channels in case of emergency such as staff absence.
- Parents/carers and students will be informed of any official PGS social media use, along with expectations for safe use and PGS action taken to safeguard the community.
- Public communications on behalf of PGS will, where possible, be read and agreed by at least one other colleague.
- PGS will ensure that any official social media use does not exclude members of the community who are unable or unwilling to use social media channels.

### 10.5.2 Personal use

Personal use is that made via personal social media accounts.

- Personal use of social networking, social media and personal publishing sites will be discussed with all members of staff as part of staff induction (safeguarding training) and will be revisited and communicated via regular staff training opportunities.
- Safe and professional behaviour will be outlined for all staff (including volunteers) as part of PGS's Staff Code of Conduct.
- Staff should not Invite, accept or engage in communications with children from the school community in any personal social media whilst in employment at Poole Grammar School
- Staff should not accept any current student of any age or any ex-student of the school under the age of 18 as a friend, follower, subscriber or similar on any personal social media account. Any pre-existing relationships or exceptions that may compromise this will be discussed with the lead DSL/Senior Leadership Team.
- If ongoing contact with students is required once they have left PGS's roll, then members of staff will be expected to use existing alumni networks or use official PGS provided communication tools.
- All communication between staff and members of the PGS community on PGS business will take place via official approved communication channels (such as PGS email addresses or phone numbers). Staff must not use personal accounts or information to make contact with students or parents, nor should any contact be accepted, except in circumstances whereby prior approval has been given by the Headteacher.
- Any communication from students/parents received on personal social media accounts will be reported to a DSL.
- Information that staff have access to as part of their employment, including photos and personal information about students and their family members, colleagues etc. will not be shared or discussed on personal social media sites.



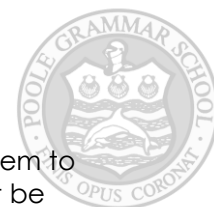
- All members of staff are strongly advised to safeguard themselves and their privacy when using social media sites. This will include being aware of location sharing services, setting the privacy levels of their personal sites as strictly as they can, opting out of public listings on social networking sites, logging out of accounts after use and keeping passwords safe and confidential.
- All members of staff are encouraged to carefully consider the information, including text and images, they share and post online and should ensure that their social media use is compatible with their professional role, in accordance with PGS's policies (safeguarding, confidentiality, data protection etc.) and the wider professional and legal framework.
- Members of staff will be encouraged to manage and control the content they share and post online. Advice will be provided to staff via staff training and by sharing appropriate guidance and resources on a regular basis.
- Members of staff will notify the Senior Leadership Team immediately if they consider that any content shared or posted via any information and communications technology, including emails or social networking sites conflicts with their role in PGS.
- Members of staff are encouraged not to identify themselves as employees of PGS on their personal social networking accounts. This is to prevent information on these sites from being linked with PGS and also to safeguard the privacy of staff and the wider PGS community.
- Members of staff will ensure that they do not represent their personal views as that of PGS on social media.
- PGS email addresses will not be used for setting up personal social media accounts.
- Members of staff who follow/like PGS's social media channels will be advised to use dedicated professional accounts where possible to avoid blurring professional boundaries.

### 10.5.3 Students use of social media

- Students will be advised to consider the risks of sharing personal details of any kind on social media sites which may identify them and / or their location. Examples would include real/full name, address, mobile or landline phone numbers, school attended, Instant messenger contact details, information through photographs, email addresses, full names of friends/family, specific interests and clubs etc.
- Students will be advised not to meet any online friends without a parent/carer or other responsible adult's permission and only when they can be present.
- Students will be advised on appropriate security on social media sites and will be encouraged to use safe and passwords, deny access to unknown individuals and be supported in learning how to block and report unwanted communications.
- Students will be encouraged to approve and invite known friends only on social networking sites and to deny access to others by making profiles private/protected.
- Parents will be informed of any official social media use with students and written parental consent will be obtained, as required.
- Any official social media activity involving students will be moderated by PGS where possible.
- PGS is aware that many popular social media sites state that they are not for children under the age of 13, therefore, PGS will not create accounts within the school specifically for students under this age.
- Any concerns regarding students' use of social networking, social media and personal publishing sites, both at home and at PGS, will be dealt with in accordance with existing PGS policies including anti-bullying and behaviour. Concerns will be raised with their parents/carers, particularly when concerning any underage use of social media sites.

### 10.5.4 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



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.

## 10.6 Digital and Video Images

This section should be read in conjunction with the school policy on "Taking, Using And Storing Images Of Students".

The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm (select/delete as appropriate):

- the school may use live-streaming or video-conferencing services in line with national and local safeguarding guidance / policies
- when using digital images, staff will inform and educate students about the risks associated with the taking, use, sharing, publication and distribution of images.
- Only school devices may be used to take images of students
- 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 such use is not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published/made publicly available on social networking sites, nor should parents/carers comment on any activities involving other students in the digital/video images
- staff and volunteers are allowed to take digital/video images to support educational aims, but must follow school policies concerning the sharing, storage, distribution and publication of those images
- care should be taken when sharing digital/video images that students are appropriately dressed
- students must not take, use, share, publish or distribute images of others without their permission
- photographs published on the website, or elsewhere that include students will be selected carefully and will comply with Online Safety Policy
- students' 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 in accordance with the school policy on Taking Storing and Using Images of Students
- images will be securely stored in line with the school retention policy
- students' work can only be published with the permission of the learner and parents/carers.

## 10.7 Online Publishing

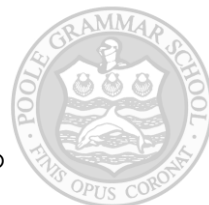
The school communicates with parents/carers and the wider community and promotes the school through:

- Public-facing website
- Social media
- Online newsletters

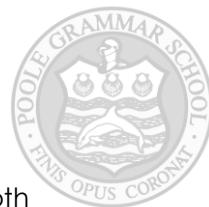
The school ensures that online safety policy has been followed in the use of online publishing e.g., use of digital and video images, copyright, identification of young people, publication of school calendars and personal information – ensuring that there is least risk to members of the school community,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

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

The school public online publishing 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 an online reporting process for parents and the wider community to register issues and concerns to complement the internal reporting process.



## 11. Appendix 1: Technology acceptable use agreement for students

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

Poole Grammar School understands the benefits technology can have on enhancing the curriculum and student's learning; however, we must ensure that students respect school property and use technology appropriately. To achieve this, we have created this acceptable use agreement which outlines our expectations of students when using technology, whether this is on personal or school devices and on or off the school premises.

This acceptable use agreement is intended to ensure:

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

### 11.1 For my own personal safety:

- I understand that the school will monitor my use of the systems, devices and digital communications.
- I will keep my username and password safe and secure – I will not share it, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may steal it.
- I will be aware of "stranger danger", when I am communicating on-line.
- I will not disclose or share personal information about myself or others when on-line (this could include names, addresses, email addresses, telephone numbers, age, gender, educational details, financial details etc.)
- If I arrange to meet people off-line that I have communicated with on-line, I will do so in a public place and take an adult with me.
- I will immediately report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it on-line.

### 11.2 User Accounts

- Student accounts are to be used by the assigned user for school-related and educational purposes, personal professional development and careers purposes only.
- Accessing or attempting to access another user's account is strictly prohibited.
- Students are required to take all necessary precautions to keep their account secure and must not share their personal account or password with others.

### 11.3 Use of Technology

- Students will only use school systems and devices that they have been given permission to access.
- Students must adhere to the online safety guidelines they have been taught.
- Students must not store or use personal data relating to a student or staff member for non-school related activities on School systems and devices.
- At school, during school hours students must only use the internet for school-related activities.
- Students must not attempt to download and run or install additional software on school owned devices.
- Students must delete emails from unknown senders without opening them and must not open any email attachments or links they contain.
- Students must not take, store or distribute images of any member of the school community without their permission.



- Students must behave responsibly and not interfere with teaching and learning whilst using School systems and devices.
- School systems and devices are subject to UK law. Students must not use the systems to upload, download, use, retain, distribute, create or access any electronic materials which:
  - May constitute a threat, bullying or harassment,
  - May be slanderous, abusive, indecent, obscene, racist, illegal or offensive.
  - May be a breach of copyright and/or licence provisions
  - Might gain access to restricted or unauthorised areas of the system and/or network, website or other hacking activities
- Students must not use School systems for mass unsolicited mailings, commercial activity or the dissemination of junk mail, viruses or malware.
- Students must not attempt to "hack" or gain access to permissions, resources or systems that they are not permitted to access.

#### 11.4 Personal Devices

- Direct connection to School networks of devices not supplied by the School is not permitted.
- Students with permission to use a personal device, such as a laptop must only connect to the PGSBYOD Wi-Fi network at the school. Please speak to a member of the network team for assistance.
- Personal mobile devices, such as mobile phones, tablets and media players must not be used on the school site and students must adhere to the school's mobile phone rules.
- Personal devices must not be used to record images/audio of other students or staff.

#### 11.5 Social Media

- Students will not use School devices to access personal social networking platforms
- Students must not communicate or attempt to communicate with staff members over personal social networking platforms or email.
- Students must not accept or send 'friend' or 'follow' requests from or to any staff member over personal social networking platforms
- Students must not publish any comments or posts about the school on any social networking platforms or websites which may affect the school's reputation.
- Students must not post or upload any defamatory, objectionable, copyright- infringing or private material, including images and videos of students, staff or parents, on any online website or platform.

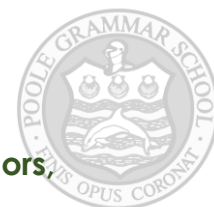
#### 11.6 Reporting Misuse

- Students will ensure that they report misuse or breaches of this agreement by students or staff members by means of the school's reporting procedure
- Violations will be dealt with in line with the relevant policy e.g. Behavioural Policy or Child Protection and Safeguarding Policy

#### 11.7 Agreement

I understand that my use of School systems and devices including the internet will be monitored. I acknowledge that I have read and understood these terms and ensure that I will abide by each principle.

<b>Name of student:</b>	
<b>Tutor Group:</b>	
<b>Signed:</b>	
<b>Date:</b>	



## 12. Appendix 2 – Technology acceptable use agreement for staff, governors, volunteers and guests

Poole Grammar School understands the benefits technology can have on enhancing the curriculum and students' learning; however, we must ensure that staff, governors, volunteers and guests use technology appropriately. To achieve this, we have created this acceptable use agreement which outlines our expectations for staff when using technology, whether this is on personal or school devices and on or off the school premises.

Please read this document carefully and sign below to accept that you agree to the terms outlined below.

### 12.1 Definitions

- Staff – Used to refer to all staff, governors, volunteers and guests
- Technology – Used to refer to all technological devices and systems

### 12.2 User Accounts

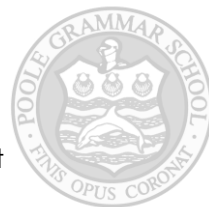
- User accounts are to be used by the assigned user / group for school related and educational purposes, personal professional development and careers purposes only.
- Accessing or attempting to access another user's account is strictly prohibited.
- Staff are required to take all necessary precautions to keep their account secure and must not share their account or password with others.

### 12.3 Use of Technology

- Staff will only use School systems and devices that they have been given permission to access.
- Staff will only use their assigned email accounts for official purposes.
- Staff will not use personal email accounts to send and receive personal data or information
- Staff will not share sensitive personal data with any other staff, students or third parties unless explicit consent has been received.
- Staff will ensure that any personal data is stored in line with the UK GDPR.
- Staff must delete emails from unknown senders without opening them and must not open any email attachments or links they contain.
- During school hours staff must only use the internet for school related activities.
- Staff must not attempt to download and run or install additional software on school owned devices.
- Staff will not store data on removable media.
- School systems and devices are subject to UK law. Staff must not use the systems to upload, download, use, retain, distribute, create or access any electronic materials which:
  - May constitute a threat, bullying or harassment,
  - May be slanderous, abusive, indecent, obscene, racist, illegal or offensive.
  - May be a breach of copyright and/or licence provisions
  - Might gain access to restricted or unauthorised areas of the system and/or network, website or other hacking activities
- Staff must not use School systems for mass unsolicited mailings, commercial activity or the dissemination of junk mail, viruses or malware.
- Staff must not attempt to gain access to permissions, resources or systems that they are not permitted to access.

### 12.4 Personal Devices

- Staff will ensure that personal mobile devices are either switched off or set to silent/discrete mode during school hours, and will only make or receive calls in locations appropriate to do so.
- Staff will not use personal mobile devices to take photographs or videos of students or staff



- Direct connection to School networks of devices not supplied by the School is not permitted.
- Personal devices, such as a laptop must connect to the PGSBYOD Wi-Fi network at the school. Please speak to a member of the network team for assistance.
- Staff will ensure that any personal device that is used to access school files, systems or data is kept secure using passwords or similar protective features.
- Staff will ensure that any school data stored on personal devices is encrypted and/or pseudonymised.
- By adding school accounts to a personal device, staff consent to Mobile Device Management, giving permission for the school to erase and wipe data off the device if it is reported lost or as part of exit procedures.

### 12.5 Web and Social Media

- Staff representing the school online on websites or via school social media accounts will express neutral opinions and will not disclose any confidential information regarding the school, or any information that may affect its reputability.
- Staff will not communicate with students or parents over personal social networking sites or email. Contact with students or parents will be done through authorised channels.
- Staff must not accept or send 'friend' or 'follow' requests from or to any students or parents over personal social networking platforms
- Staff will ensure that they apply appropriate privacy settings to any social networking sites.
- Staff must not publish any comments or posts about the school on any social networking platforms or websites which may affect the school's reputation.
- Staff must not post or upload any defamatory, objectionable, copyright-infringing or private material, including images and videos of students, staff or parents, on any online website or platform.
- In line with the above, staff will only post images or videos of students, staff or parents for the activities for which consent has been sought.

### 12.6 Training

- Staff will ensure they participate in any online safety training offered to them, and will remain up-to-date with current developments in social media and the internet as practical.
- Staff will ensure they employ methods of good practice and act as a role model for students when using technology.

### 12.7 Reporting Misuse

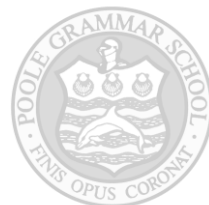
- Staff will ensure that they adhere to any responsibility they have for monitoring students use of technology.
- Staff will ensure that they report misuse or breaches of this agreement by students or staff members by means of the school's reporting procedure
- Staff understand that violations to this agreement will be dealt with in line with the relevant policy and that disciplinary action may be taken in accordance with the Disciplinary Policy and Procedures.

### 12.8 Agreement

I understand that my use of School systems and devices including the internet will be monitored. I acknowledge that I have read and understood these terms and ensure that I will abide by each principle.

<b>Name:</b>	
<b>Signed:</b>	
<b>Date:</b>	





### 13. Appendix 3 – Log sheets

#### 13.1 Record of reviewing devices

Student name:

Group: .....

Date: .....

Reason for investigation: .....

.....

.....

.....

#### Details of first reviewing person

Name: .....

Position: .....

Signature: .....

#### Details of second reviewing person

Name: .....

Position: .....

Signature: .....

Device	Reason for concern

Conclusion and Action proposed or taken

.....

.....

.....

.....



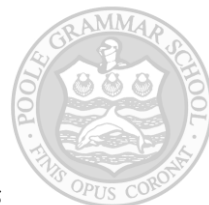
### 13.2 Filtering change request

(An email to the Network Team and Online Safety Lead will suffice but this form highlights details required).

Member of staff requesting change:	
Type of change	<input type="checkbox"/> Remove from filter list <input type="checkbox"/> Add to filter list
Keyword/URL request:	
Reason for change request:	

Submit form to Online Safety Lead

OSL/DSL/SLT response:  <i>(This request will be considered by at least two members of senior staff)</i>	
Network team response:	



### 13.3 Online Safety Incident report form

(An email to the Network Team and Online Safety Lead will suffice but this form highlights details required).

Any member of the school community can raise a concern about an online safety incident. If you have witnessed or experienced an incident please complete the form below to help us to address the issue. It is important that you provide as much detail as possible. Once completed please hand this report to Mr Chase.

Name of person reporting incident:			
Signature:			
Date you are completing this form:			
Where did the incident take place:	Inside school?		Outside school?
Date of incident(s):			
Time of incident(s):			

Who was involved in the incident(s)?	Full names and/or contact details
Children/young people	
Staff member(s)	
Parent(s)/carer(s)	
Other, please specify	

Type of incident(s) (indicate as many as apply)			
Accessing age inappropriate websites, apps and social media		Accessing someone else's account without permission	
Forwarding/spreading chain messages or threatening material		Posting images without permission of all involved	
Online bullying or harassment (cyber bullying)		Posting material that will bring an individual or the school into disrepute	
Racist, sexist, homophobic, religious or other hate material		Online gambling	
Sexting/Child abuse images		Deliberately bypassing security	
Grooming		Hacking or spreading viruses	
Accessing, sharing or creating pornographic images and media		Accessing and/or sharing terrorist material	
Accessing, sharing or creating violent images and media		Drug/bomb making material	
Creating an account in someone else's name to bring them into disrepute		Breaching copyright regulations	



Type of incident(s) (indicate as many as apply)	
Other breach of acceptable use agreement, please specify	

Full description of the incident	What, when, where, how?
Name all social media involved	Specify: Twitter, Facebook, Whatsapp, Snapchat, Instagram etc
Evidence of the incident	Specify any evidence available but do not attach.



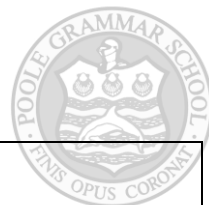
### 13.4 Online Safety Incident Record

This form will be completed by the Online Safety Lead as a record of an incident; it may be completed in place of the report form if one hasn't been submitted.

Name of person reporting incident:			
Date of report:			
Where did the incident take place:	Inside school?		Outside school?
Date of incident(s):			
Time of incident(s):			

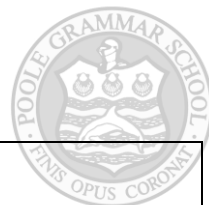
Who was involved in the incident(s)?	Full names and/or contact details
Children/young person	
Staff member(s)	
Parent(s)/carer(s)	
Other, please specify	

Type of incident(s) (indicate as many as apply)			
Accessing age inappropriate websites, apps and social media		Accessing someone else's account without permission	
Forwarding/spreading chain messages or threatening material		Posting images without permission of all involved	
Online bullying or harassment (cyberbullying)		Posting material that will bring an individual or the school into disrepute	
Racist, sexist, homophobic, religious or other hate material		Online gambling	
Sexting/Child abuse images		Deliberately bypassing security	
Grooming		Hacking or spreading viruses	
Accessing, sharing or creating pornographic images and media		Accessing and/or sharing terrorist material	
Accessing, sharing or creating violent images and media		Drug/bomb making material	
Creating an account in someone else's name to bring them into disrepute		Breaching copyright regulations	
Other breach of Acceptable Use Agreement			
Other, please specify			



Full description of the incident	What, when, where, how?
Name all social media involved	Specify: Twitter, Facebook, Whatsapp, Snapchat, Instagram etc
Evidence of the incident	Specify any evidence provided but do not attach

Immediate action taken following the reported incident:	
Incident reported to Online Safety Lead/DSL/Deputy DSL/Head of Year/Headteacher	
Safeguarding advice sought, please specify	
Referral made to First Response Hub	
Incident reported to police and/or CEOP	
Online safety policy to be reviewed/amended	
Parent(s)/carer(s) informed please specify	
Incident reported to social networking site	
Other actions e.g. warnings, sanctions, debrief and support	



Response in the wider community e.g. letters, newsletter item, assembly, curriculum delivery

**Brief summary of incident, investigation and outcome (for monitoring purposes)**

Empty box for the brief summary of incident, investigation and outcome.



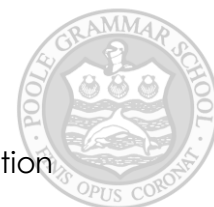
## 14. Appendix 4 - Procedures for Responding to Specific Online Incidents or Concerns

### 14.1 Responding to concerns regarding Youth Produced Sexual Imagery ("Sexting")

**PGS** recognises youth produced sexual imagery (known as "sexting") as a safeguarding issue; all concerns will be reported to and dealt with by the DSL or Online Safety Lead (or deputy DSL).

- We will follow the advice as set out in the non-statutory UKCCIS/DfE guidance: 'Sharing nudes and semi-nudes'.
- PGS will ensure that all members of the community are made aware of the potential social, psychological and criminal consequences of 'sexting' by implementing preventative approaches, via a range of age and ability appropriate educational methods.
- We will ensure that all members of the community are aware of sources of support regarding youth produced sexual imagery.
- We will respond to concerns regarding youth produced sexual imagery, regardless of whether the incident took place on site or using school provided or personal equipment.
- We will not:
  - View any images suspected of being youth produced sexual imagery, unless there is no other possible option, or there is a clear need or reason to do so;
    - If it is deemed necessary, the image will only be viewed by the DSL (or deputy DSL) and their justification for viewing the image will be clearly documented;
  - Send, share, save or make copies of content suspected to be an indecent image of a child (i.e. youth produced sexual imagery) and will not allow or request students to do so.
- If made aware of an incident involving the creation or distribution of youth produced sexual imagery, we will:
  - Act in accordance with our child protection policies and the relevant **Pan-Dorset Safeguarding Children Partnership's** procedures;
  - Ensure the DSL (or deputy) responds in line with the UKCCIS/DfE guidance 'Sharing nudes and semi-nudes';
  - Store the device securely;
- If an indecent image has been taken or shared on our network or devices, we will act to block access to all users and isolate the image.
  - Carry out a risk assessment which considers any vulnerability of students involved, including carrying out relevant checks with other agencies;
  - Inform parents/carers, if appropriate, about the incident and how it is being managed;
  - Make a referral to **BCP First Reponse Hub or Dorset Children's Advice and Duty Service** and/or the Police, as deemed appropriate in line with the UKCCIS/DfE guidance 'Sharing nudes and semi-nudes';
  - Provide the necessary safeguards and support for students, such as offering counselling or pastoral support;
  - Implement appropriate sanctions in accordance with our behaviour policy but taking care not to further traumatise victims where possible;
  - Consider the deletion of images in accordance with the UKCCIS/DfE guidance: 'Sharing nudes or semi-nudes';
  - Images will only be deleted once the DSL has confirmed that other agencies do not need to be involved; and are sure that to do so would not place a child at risk or compromise an investigation.
- Review the handling of any incidents to ensure that best practice was implemented; the Senior Leadership Group will also review and update any management procedures, where necessary.



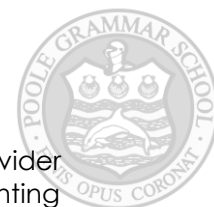


#### 14.2 Responding to concerns regarding Online Child Sexual Abuse and Exploitation (including child criminal exploitation)

- **PGS** will ensure that all members of the community are aware of online child sexual abuse, including: exploitation and grooming; the consequences; possible approaches which may be employed by offenders to target children and how to respond to concerns.
- **PGS** recognises online child sexual abuse and exploitation (including criminal exploitation) as a safeguarding issue and, as such, all concerns will be reported to and dealt with by the DSL (or deputy).
- We will implement preventative approaches for online child sexual abuse and exploitation (including criminal exploitation) via a range of age and ability appropriate education for students, staff and parents/carers.
- We will ensure that all members of the community are aware of the support available regarding online child sexual abuse and exploitation (including criminal exploitation), both locally and nationally.
  - We will ensure that the 'Click CEOP' report button used to report online child sexual abuse is visible and available to students and other members of our community on internal PGS websites.
- If made aware of an incident involving online child sexual abuse and exploitation (including criminal exploitation), we will:
  - Act in accordance with our child protection policies and the relevant Pan-Dorset Safeguarding Children Partnership's procedures;
  - If appropriate, store any devices involved securely;
  - Make a referral to the BCP First Response Hub or Dorset Children's Advice and Duty Service (if required/appropriate) and immediately inform Dorset police via 101, or 999 if a child is at immediate risk;
  - Carry out a risk assessment which considers any vulnerabilities of student(s) involved (including carrying out relevant checks with other agencies);
  - Inform parents/carers about the incident and how it is being managed;
  - Provide the necessary safeguards and support for students, such as, offering counselling or pastoral support;
  - Review the handling of any incidents to ensure that best practice is implemented; leadership team will review and update any management procedures, where necessary.
- We will respond to concerns regarding online child sexual abuse and exploitation (including criminal exploitation), regardless of whether the incident took place on our premises or using school provided or personal equipment.
  - Where possible, students will be involved in decision making and if appropriate, will be empowered to report concerns such as via the Click CEOP report: [www.ceop.police.uk/safety-centre/](http://www.ceop.police.uk/safety-centre/)
  - If we are unclear whether a criminal offence has been committed, the DSL (or deputy) will obtain advice immediately through the BCP First Response Hub or Dorset Children's Advice and Duty Service and/or Dorset Police.
- If made aware of intelligence or information which may relate to child sexual exploitation (on or offline), it will be passed through to the BCP First Response Hub or Dorset Children's Advice and Duty Service by the DSL (or deputy).
- If students at other setting are believed to have been targeted, the DSL (or deputy) will seek support from Dorset Police and/or the BCP First Response Hub or Dorset Children's Advice and Duty Service first to ensure that potential investigations are not compromised.

#### 14.3 Responding to concerns regarding Indecent Images of Children (IIOC)

- **PGS** will ensure that all members of the community are made aware of the possible consequences of accessing Indecent Images of Children (IIOC).
- We will respond to concerns regarding IIOC on our equipment and/or personal equipment, even if access took place off site.



- We will seek to prevent accidental access to IIOC by using an Internet Service provider (ISP) which subscribes to the Internet Watch Foundation block list and by implementing appropriate filtering, firewalls and anti-spam software.
- If we are unclear if a criminal offence has been committed, the DSL (or deputy) will obtain advice immediately through Dorset Police and/or the BCP First Response Hub or Dorset Children's Advice and Duty Service.
- If made aware of IIOC, we will:
  - Act in accordance with our child protection policy and the relevant Pan-Dorset Safeguarding Children Partnership's procedures;
  - Store any devices involved securely;
  - Immediately inform appropriate organisations, such as the Internet Watch Foundation (IWF), Dorset police.
- If made aware that a member of staff or a student has been inadvertently exposed to indecent images of children, we will:
  - Ensure that the DSL (or deputy) is informed;
  - Ensure that the URLs (webpage addresses) which contain the suspect images are reported to the Internet Watch Foundation via [www.iwf.org.uk](http://www.iwf.org.uk) ;
  - Ensure that any copies that exist of the image, for example in emails, are deleted;
  - Report concerns, as appropriate to parents/carers.
- If made aware that indecent images of children have been found on school provided devices, we will:
  - Ensure that the DSL (or deputy) is informed;
  - Ensure that the URLs (webpage addresses) which contain the suspect images are reported to the Internet Watch Foundation via [www.iwf.org.uk](http://www.iwf.org.uk) ;
  - Ensure that any copies that exist of the image, for example in emails, are deleted.
  - Inform the police via 101 (999 if there is an immediate risk of harm) and BCP First Response Hub or Dorset Children's Advice and Duty Service (as appropriate);
  - Only store copies of images (securely, where no one else has access to them and delete all other copies) at the request of the police only;
  - Report concerns, as appropriate to parents/carers.
- If made aware that a member of staff is in possession of indecent images of children on school provided devices, we will:
  - Ensure that the Headteacher is informed in line with our managing allegations against staff policy;
  - Inform the Local Authority Designated Officer (LADO) and other relevant organisations in accordance with our managing allegations against staff policy;
  - Quarantine any devices until police advice has been sought.

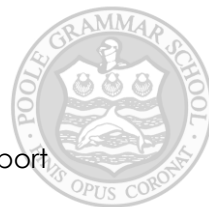
#### 14.4 Responding to concerns regarding radicalisation or extremism online

- **PGS** will take all reasonable precautions to ensure that students are safe from terrorist and extremist material when accessing the Internet in school and that suitable filtering is in place which takes into account the needs of students.
- When concerns are noted by staff that a student may be at risk of radicalisation online then the Prevent Lead, DSL or deputy DSL will be informed immediately and action will be taken in line with PGS's Safeguarding policy.
- If we are concerned that staff may be at risk of radicalisation online, the Headteacher will be informed immediately, and action will be taken in line with the child protection and allegations policies.

#### 14.5 Responding to concerns regarding cyberbullying

Cyberbullying, along with all other forms of bullying, of any member of the PGS's community will not be tolerated. Full details are set out in PGS policies regarding anti-bullying and behaviour.

- All incidents of online bullying reported will be recorded.

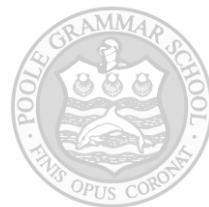


- There are clear procedures in place to investigate incidents or allegations and support anyone in the PGS community affected by online bullying.
- If **PGS** is unclear if a criminal offence has been committed, then the DSL will obtain advice immediately through the BCP First Response Hub and/or Dorset Police.
- Students, staff and parents/carers will be advised to keep a record of the bullying as evidence.
- **PGS** will take steps to identify the bully where possible and appropriate. This may include examining PGS system logs, identifying and interviewing possible witnesses, and contacting the service provider and the police, if necessary.
- Students, staff and parents/carers will be required to work with PGS to support the approach to cyberbullying and PGS's online-safety ethos.
- Sanctions for those involved in online or cyberbullying may include the following:
  - Those involved being asked to remove any material deemed to be inappropriate or offensive.
  - A service provider being contacted to remove content if those involved refuse to or are unable to delete content.
  - Internet access may be suspended at PGS for the user for a period of time. Other sanctions for students and staff may also be used in accordance to PGS's anti-bullying, behaviour policy or Acceptable Use Agreement.
  - Parent/carers of students involved in online bullying will be informed.
  - The Police will be contacted if a criminal offence is suspected.

#### 14.6 Responding to concerns regarding Online Hate

Online hate content, directed towards or posted by, specific members of the community will not be tolerated at PGS and will be responded to in line with existing policies, including anti-bullying and behaviour.

- All members of the community will be advised to report online hate in accordance with relevant policies and procedures.
- The Police will be contacted if a criminal offence is suspected.
- If we are unclear on how to respond, or whether a criminal offence has been committed, the DSL (or deputy) will obtain advice through the BCP First Response Hub and/or Dorset Police.



## 15. Appendix 5 - Equality Impact Assessment (EQIA)

Document Name: Online Safety Policy

Evidence:

What evidence have you considered?	
Disability	Exceptions will be made to this policy where a student with SEND has a specific requirement (such as accessibility features or those required for medical monitoring e.g. blood sugar levels monitored by mobile phone). Specific additional provisions are made for SEND students, due to a general increased risk online.
Sex	Has no impact on this policy.
Race	Has no impact on this policy.
Age	Has no impact on this policy.
Gender Reassignment	Has no impact on this policy.
Sexual Orientation	Has no impact on this policy.
Religion or Belief	Has no impact on this policy.
Pregnancy or Maternity	Has no impact on this policy.
Carers	Has no impact on this policy.
Socio-economic	Has no impact on this policy.

### Engagement and Involvement

Where appropriate, we have consulted:

	<input checked="" type="checkbox"/> or <input checked="" type="checkbox"/>	Comments
Trustees	<input checked="" type="checkbox"/>	Pending full governing board review
Parents	<input checked="" type="checkbox"/>	
Students	<input checked="" type="checkbox"/>	
Staff	<input checked="" type="checkbox"/>	Key staff have been consulted on systems in place
Other	<input checked="" type="checkbox"/>	

Overall impact	Whole school
Action to be taken	Any requests regarding filtering on school devices will be considered with due regard to the protected characteristics; exceptions will be made for SEND students, where for example adaptations are required (for example, accessibility aids or medical monitoring using personal devices).

**Assessment undertaken by:**

**Nathan Chase**

**Position:**

**Assistant Headteacher**

**Date assessment undertaken:**

**September 2023**