THE PORTSMOUTH GRAMMAR SCHOOL

The PGS Online Safety Policy

Contents

The PGS Online Safety Policy

1. Introduction

1.1. This policy applies to all members of The Portsmouth Grammar School community who have access to and are users of school ICT systems, either in or out of the school. The school acknowledges that it has a responsibility to educate the pupils and staff to use information and communication technologies in a safe and responsible way, developing skills in managing personal online profiles and ensuring the safeguarding of all users at an age-appropriate level.

2. Development, Monitoring and Review of this Policy

2.1. This Online Safety Policy has been developed by the Online Safety Committee consisting of the Deputy Head (Pastoral), Senior Deputy Head, Deputy Head of the Junior School, the Head of ICT Services, Computing Leader (JS), Assistant Head (Pastoral) (JS), Head of Pastoral Curriculum (SS), Digital Learning Leader (JS), Head of Digital Learning (SS) and the Deputy Head (Teaching and Learning) (SS). The policy is reviewed every year by the Governing Body and is available on the school website.

3. Schedule for Development, Monitoring and Review

3.1. The school monitors the impact of the policy, using logs of reported incidents and dialogue with the school community. This information is reported to Governors via the annual ICT and Data Report. As well as scheduled reviews, the policy will also be updated to reflect the latest guidance and recommended practice whenever necessary.

4. Scope of the Policy

4.1. The Education and Inspections Act 2006 empowers the Head to such extent as is reasonable to regulate the behaviour of pupils when they are off the school site, and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying, or other online safety incidents covered by this policy, which may take place outside of the school, but are linked to membership of the school. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data. In the case of both Acts, action can only be taken over issues covered by the published Behaviour Management Policy.

4.2. In dealing with incidents relating to online safety, the school will also make reference to the policies on Behaviour Management and Anti-bullying, and will, where known, inform parents of incidents of inappropriate online safety behaviour that take place out of school. These policies are being updated to reflect the Online Safety Act 2023 that came into force on 31st January 2024. Under Part 10, six new criminal offences have come into force which aim to address the rising concerns surrounding online harm and ensure appropriate measures are in place to protect users and prosecute offenders.

Roles and Responsibilities

The following sections outline the online safety roles and responsibilities of individuals and groups within the school.

5. Governors

5.1. Governors are responsible for the approval of the Online Safety Policy and for reviewing the effectiveness of the policy. Governors receive an annual report as part of the ICT and Data Report which includes information about online safety incidents and monitoring information.

6. The Head

6.1. The Head has a duty of care for ensuring the safety (including online safety) of members of the school community, with the day-to-day responsibility for online safety delegated to the Online Safety Committee

6.2. In the event of an online safety allegation being made against a member of staff the allegation will be investigated in line with the procedures set out for staff in the Discipline, Capability & Grievance Procedure and, in the case of a serious allegation, in the Safeguarding and Child Protection Policy and Procedure

6.3. Monitoring and support of those in school who carry out the internal online safety monitoring role is conducted through the 360-degree safe online safety appraisal; this is to provide an audit of existing practice and also to support those colleagues who take on important monitoring roles. This may also involve an external audit commissioned by the Governing Body

6.4. The Senior Management Team receive regular monitoring reports from the Online Safety Officers (whose role is described below) each term.

7. Online Safety Officers

The Portsmouth Grammar School has chosen to combine the responsibility for online safety with the Designated Safeguarding Lead role. In the Senior School the Deputy Head (Pastoral) has responsibility for online safety, and in the Junior School, the Deputy Head. They will collectively:

7.1. Lead the Online Safety Committee

7.2. Take day-to-day responsibility for online safety issues and have a leading role in establishing and reviewing the school Online Safety Policy and related documentation

7.3. Ensure that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place, as well as an understanding of the expectations, roles and responsibilities in relation to filtering and monitoring

7.4. Provide training and advice on online safety for staff as required, and at least annually

7.5. Liaise with school technical staff

7.6. Receive reports of online safety incidents and liaise with the Head of ICT Services on the log of incidents to inform future online safety developments

7.7. Generate the information for the annual ICT and Data Report for Governors which will include current issues and associated monitoring logs

7.8. Report regularly to the Senior Management Team

7.9. Lead a biannual review of the efficacy of the school's filtering and monitoring.

8. Head of ICT Services

The Head of ICT Services is responsible for ensuring that:

8.1. The school's technical infrastructure is secure and is not open to misuse or malicious attack

8.2. The school meets required online safety technical requirements, complying with the Department for Education's filtering and monitoring standards

8.3. Users may only access the networks and devices through a properly enforced policy outlined in the ICT Services Handbook which stipulates that dual factor authentication is in use by staff to protect the integrity and security of IT systems

8.4. The school has the necessary filters in place which filter content at an age appropriate level and reviews these every two years in conjunction with the Senior Deputy Head (SS) and the Deputy Head (JS)

8.5. They keep up to date with online safety technical information in order to effectively carry out their online safety role and to inform and update others as relevant

8.6. The use of all ICT is regularly monitored at The Portsmouth Grammar School in order that any misuse or attempted misuse can be reported to the Senior Deputy or Head

8.7. Monitoring software and systems are implemented and updated

8.8. Information is handled in accordance with the Data Protection Policy and the necessary encryption is in place.

9. Teaching and Support Staff

Teaching and Support Staff are responsible for ensuring that:

9.1. They have an up-to-date awareness of online safety matters and comply with the current school online safety policy and practices

9.2. They have read and understood The PGS Staff Social Media and Digital Images Policy and associated guidance provided by the school

9.3. They have read, understood, and signed the Staff Acceptable Use Policy (AUP)

9.4. They report any suspected misuse or problem to the Senior Deputy or Deputy Head of the Junior School

9.5. They understand and follow the guidance on digital communications with pupils and parents provided in the Common Room Handbook and the PGS Code of Professional Conduct for Staff.

9.6. Online safety issues are included at relevant points in the curriculum and other activities

9.7. Pupils understand and follow the Online Safety and Acceptable Use policies in lessons and other school activities

9.8. Pupils have an appropriate understanding of research skills and the need to avoid plagiarism and uphold copyright regulations

9.9. They monitor the use of digital technologies, mobile devices, cameras etc in lessons and other school activities

9.10. In lessons where internet use is pre-planned, pupils should be guided to sites checked as suitable for their use and if unsuitable material is found, the Head of ICT Services should be notified

9.11. If inappropriate content is found during the course of a lesson with Junior School pupils, the pupil's Form Teacher and parents should also be notified.

10. Online Safety Committee

10.1. The Online Safety Committee provides a consultative group that has wide representation from the school community, with responsibility for issues regarding online safety and the monitoring of the Online Safety Policy including the impact of initiatives.

10.2. Members of the Online Safety Committee will assist with:

10.3. The production, review and monitoring of the school Online Safety Policy and related documentation

10.4. The production, review and monitoring of the school filtering procedures and requests for filtering changes, and the content included in policies applied by Schools Mobile (which parents may choose to adopt)

10.5. Mapping and reviewing the online safety curricular provision – ensuring relevance, breadth and progression

10.6. Monitoring network and online safety incident logs

10.7. Consulting stakeholders – including parents and the pupils about the online safety provision

10.8. Monitoring improvement actions identified through use of the 360 degree safe self-review tool

10.9. Engaging with Pupil Councils and Parents' Forums on matters of online safety.

11. Pupils

Pupils:

11.1. Are responsible for using the school digital technology systems in accordance with the Pupil Acceptable Use Policy (subject to pupil signature from Year 3 upwards)

11.2. Have an appropriate understanding of research skills and the need to avoid plagiarism and uphold copyright regulations

11.3. Need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so

11.4. Are expected to know and understand policies and expectations on the use of mobile devices and digital cameras. They should also know and understand policies and guidance on the taking and use of images and film of other members of the community and on anti-bullying, at an age-appropriate level

11.5. Have an appropriate understanding of the importance of adopting good online safety practice when using digital technologies out of school and realise that the school's Online Safety Policy covers their actions out of school, if related to their membership of the school.

12. Parents

12.1. Parents play a crucial role in ensuring that their children understand the need to use the internet and mobile devices in an appropriate way.

12.2. The school will take opportunities to help parents understand these issues through parents' information evenings, newsletters, the parent portal and information about online safety campaigns and literature. Parents are encouraged to support the school in promoting good online safety practice through filtering and monitoring the online use of young people as well as to follow guidelines on the appropriate use of:

12.2.1. Digital images and video taken at school events

12.2.2. The parent portal

12.2.3. Their children's personal devices in the school (where these are allowed).

Policy Statements

13. Education – Pupils

13.1. Whilst regulation and technical solutions are very important, including that of Schools Mobile where parents choose to adopt it, their use must be balanced by educating pupils to take a responsible approach. The education of pupils in online safety is, therefore, an essential part of the school's online safety provision in ensuring they avoid online safety risks and build their resilience.

13.2. At The Portsmouth Grammar School, the emphasis of online safety is on promoting good behaviour and responsible practice giving consideration to young people's online exposure to content, contact, conduct and commerce. The school actively participates in national online safety events e.g. safer internet day, and the online safety curriculum is broad, relevant and provides progression, with opportunities for creative activities and is provided in the following ways:

13.2.1. A planned online safety curriculum is provided as part of Computing & PSHE lessons (Junior School) and the Computing and Pastoral Curriculum lessons (Senior School)

13.2.2. Key online safety messages are reinforced as part of a planned programme of assemblies and special events, including highlighting harmful online content and challenges

13.2.3. Pupils are taught in all lessons to be critically aware of the materials and content they access online and be guided to validate the accuracy of information at an age-appropriate level

13.2.4. Pupils are taught at an appropriate age to acknowledge the source of information used and to respect copyright when using material accessed on the internet

13.2.5. Pupils are helped to understand the need for the Pupil Acceptable Use Policy through an annual, whole-school sign up procedure in the Autumn term through which they are encouraged to adopt safe and responsible use both within and outside school through the Pastoral Curriculum

13.2.6. Staff act as good role models in their use of digital technologies, the internet and mobile devices

13.2.7. In lessons where internet use is planned, it is best practice that pupils should be guided to sites checked as suitable for their use

13.2.8. Where pupils are allowed freely to search the internet in lessons, staff are vigilant in monitoring the content of the websites visited

13.2.9. It is accepted that from time to time, for good educational reasons, pupils may need to research topics (e.g. racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that Helpdesk@pgs.org.uk temporarily remove those sites from the filtered list for the period of study. Any such request may require confirmation first from the Deputy Head (Pastoral).

14. Education & Training – Staff and Volunteers

14.1. Academic staff receive annual online safety training and understand their roles and responsibilities, including in relation to filtering and monitoring.

14.2. Regular online safety training is made available to staff via online external and internal modules.

14.3. An audit of the online safety training needs of all staff is carried out annually in the summer term to identify any areas of concern as part of ongoing feedback on internal staff CPD.

14.4. All new staff receive online safety training as part of their induction programme, ensuring that they fully understand the school Online Safety Policy, Acceptable Use Policies and associated policies and guidance

14.5. This Online Safety Policy and its updates are presented to and discussed by staff when appropriate

14.6. The Online Safety Officers provide advice, guidance and training to individuals as required.

15. Training – Governors

Governors are required to develop an awareness of the issues relating to online safety at the school. This will be achieved in a number of ways:

15.1. Information provided through the annual report, including assurance that appropriate filtering and monitoring systems are in place

15.2. Briefings from members of staff who are invited to attend Governing Body meetings

15.3. Attendance at training provided by relevant organisations

15.4. Participation in school training for staff or information sessions for parents

16. Technical – infrastructure / equipment, filtering and monitoring

16.1. School technical systems are managed in ways that ensure that the school meets recommended technical requirements e.g. in line with the Department for Education's filtering and monitoring standards

16.2. There are regular reviews and audits of the safety and security of school technical systems

16.3. Servers, wireless systems and cabling are securely located and physical access restricted

16.4. All users have clearly defined access rights to school technical systems and devices

16.5. All users are provided with a username and secure password by the IT Services department who keep an up to date record of users and their usernames. Users are responsible for the security of their username and password and staff are required to use two factor authentication, in line with the ICT Services Handbook advice

16.6. The "administrator" passwords for the school ICT system, used by the Head of ICT Services are also available to the Head and kept in a secure place

16.7. The Head of ICT Services is responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations

16.8. Internet access is filtered for all users. Illegal content is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list

16.9. Content lists are regularly updated and internet use is logged and regularly monitored. There is a clear process in place to deal with requests for filtering changes

16.10. The school provides differentiated user-level filtering

16.11. School technical staff regularly monitor and record the activity of users on the school technical systems and users are made aware of this in the Acceptable Use Policies

16.12. Users report any security breach(es) to Helpdesk@pgs.org.uk or the Head of ICT Services

16.13. Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, workstations, mobile devices etc. 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 anti-virus software

16.14. An agreed protocol is in place for the provision of temporary access of "guests" (e. g. trainee teachers, supply teachers, visitors) on to the school systems.

17. Use of digital and video images

Please refer to The PGS Staff Social Media and Digital Images Policy.

18. Protection

The School has the appropriate level of security measures and procedures in place in order to safeguard their systems, staff and pupils. These have taken into consideration the cyber security standards for schools and colleges. The effectiveness of these procedures are reviewed bi-annually. Please refer to the PGS Data Protection Notice and the PGS Data Protection Policy.

19. Communications

A wide range of rapidly developing communications technologies has the potential to enhance learning. The following table shows how the school considers that the benefits of using these technologies for education outweighs their risks:

	Staff and other adults				Pupils			
Communication Technologies	Allowed	Allowed at Certain Times	Allowed for selected	Not Allowed	Allowed	Allowed at Certain Times	Allowed with Staff Permission	Not Allowed
Mobile phones may be brought to school	✓				✓*			
Use of mobile phones in lessons		✓					✓[5]	✓[2]
Taking photos on mobile phones / cameras	✓[1]						✓[1]	✓[4]
Use of other mobile devices eg tablets, gaming devices	✓						✓[1]	✓[2]
Use of personal email addresses in school, or on school network	✓					✓[1]		✓[2]
Use of school email for personal emails				✓		✓[1]		✓[2]
Use of messaging apps		✓[3]				✓[3]		

[1] See PGS Social Media and Digital Images Policy

Use of social media		✓				✓[1]		✓[2]
Use of blogs		✓					✓[1]	✓[2]
Use of tablets to access the internet	✓						✓[6]	

*from Year 3 and over [1]Senior School [2] Junior School [3]Selected software
[4]Junior School and Middle School [5]Yr 9 and above only [6]Only through school network not through 3G and 4G internet access

19.1. 19.1When using communication technologies, the school considers the following as good practice:

19.1.1. Users must immediately report to the Senior Deputy (SS) or Deputy Head (JS) 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

19.1.2. Any digital communication between staff and pupils or parents must be professional in tone and content. These communications may only take place on official (monitored) school systems. Social media, unless registered with the Deputy Head (Innovation) or the Head of the Junior School, must not be used for these communications

19.1.3. Pupils at KS3 and above will be provided with individual school email addresses for educational use

19.1.4. Pupils should be taught about online safety issues, such as the risks attached to the sharing of personal details. They should also be taught strategies to deal with inappropriate communications and be reminded of the need to communicate appropriately when using digital technologies

19.1.5. Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff.

20. Social Media - Protecting Professional Identity

20.1. Staff are aware of and adhere to The PGS Staff Social Media and Digital Images Policy which highlights the need to use social media responsibly and protect a user's online profile. Please refer to The PGS Staff Social Media and Digital Images Policy for further information.

21. Responding to incidents of misuse

21.1. The school will investigate any reports of inappropriate use of the school network, school equipment, and internet in line with the school's Behaviour Management Policy. Further guidance on inappropriate activities is provided to staff in the Common Room Handbook and the PGS Code of Professional Conduct for Staff.

22. Illegal Incidents

22.1. If there is any suspicion that the incident may contain child abuse images, or if there is any other suspected illegal activity, this will be reported following procedures in the Safeguarding and Child Protection Policy and Procedure. The school, where appropriate, will refer the matter to the police.

23. Other Incidents

It is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. Any incidents will be dealt with as soon as possible in a proportionate manner, making reference to The PGS Behaviour Management Policy. Examples of incidents that may occur are as follows:

23.1. Unauthorised use of non-educational sites during lessons

23.2. Unauthorised use of mobile phone, digital camera or other mobile device

23.3. Unauthorised or inappropriate use of social media, messaging apps, internet or personal email

23.4. Unauthorised downloading or uploading of files

23.5. Allowing others to access school network by sharing username and passwords

23.6. Attempting to access or accessing the school network, using another person's account

23.7. Corrupting or destroying the data of other users or causing deliberate damage to hardware or software

23.8. Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature

23.9. Actions which could bring the school into disrepute or breach the integrity of the ethos of the school

23.10. Using proxy sites or other means to subvert the school's filtering system

23.11. Accidentally accessing offensive or pornographic material and failing to report the incident

23.12. Deliberately accessing or trying to access offensive or pornographic material

23.13. Receipt or transmission of material that infringes the copyright of another person or infringes the General Data Protection Regulation

23.14. Careless use of personal data: e.g. holding or transferring data in an insecure manner

23.15. Deliberate actions to breach data protection or network security rules

23.16. Staff using personal email, personal social networking or personal instant messaging to carrying out digital communications with pupils

23.17. Actions which could compromise a staff member's privacy and/or professional standing

23.18. Breaching copyright or licensing regulations

23.19. Continued infringements of the above, following previous warnings or sanctions.

24. Associated policies and procedures

This policy should be read in conjunction with the following associated policies and guidance:

24.1. The PGS Data Protection Policy

24.2. ICT Equipment and Disposal Policy

24.3. ICT AUPs (Employees & Pupils)

24.4. The PGS Mobile Devices Policy for Pupils

24.5. Privacy Policy

24.6. The PGS Staff Social Media and Digital Images Policy

24.7. Encryption Policy

24.8. The PGS Anti-Bullying Policy

24.9. The PGS Safeguarding & Child Protection Policy and Procedure

24.10. The PGS Behaviour Management Policy

24.11. Tablet Rules for Pupils

24.12. The PGS Code of Professional Conduct for Staff

24.13. The Common Room Handbook

24.14. The PGS EYFS Camera, Mobile Phone and Recording Devices Policy.

25. Allocation of Tasks and Version Control

Allocation of Tasks

Task	Allocated to	When / frequency of review
Keeping the policy up to date and compliant with the law and best practice	Online Safety Committee	As required, and at least annually
Monitoring the implementation of the policy, relevant risk assessments and any action taken in response and evaluating effectiveness	Deputy Head (Pastoral)	As required, and at least termly
Maintaining up to date records of all information created in relation to the policy and its implementation as required by the GDPR	Deputy Head (Pastoral)	As required, and at least termly
Receiving/reviewing input from interested groups (such as pupils, staff, Parents) to consider improvements to the School's processes under the policy	Deputy Head (Pastoral)	As required, and at least annually
Formal annual review	Education Committee	Annually

Version Control

Date Approved	15th March 2024 (Governing Body)
Date Reviewed	26th January 2024 (Safeguarding Committee)
Next Review Date	Spring Term 2025
Policy author (SMT)	Deputy Head (Pastoral)
Status	External
Report	IT and Data Report

Ph4200324