E-Safety & Social Media Policy

Petty Pool

Change Control

Version	3
Date Approved by Board	
Author	Graham Hunter
Date Issued	September 2023
Review Date	July 2025

CONTENTS

PURPOSE

1.1 Petty Pool College recognises the benefits and opportunities that new technologies offer to teaching and learning. We encourage the use of technology in order to enhance skills and promote achievement. However, the accessible and global nature of the internet and the variety of technologies available mean that we are also aware of potential risks and challenges associated with such use.

Our approach is to implement safeguards within the College and to support staff and learners to identify and manage risks independently. We believe this can be achieved through a combination of security measures, training and guidance and the implementation of our associated policies. In furtherance of our duty to safeguard learners and protect them from the risk posed by extremism and radicalisation, we will do all that we can to make our learners and staff stay safe online and to satisfy our wider duty of care.

This E-Safety policy should be read in conjunction with other relevant College policies including IT Acceptable Use Policy

2. SCOPE

2.1 This policy covers:
Anyone logging into any network, service, website or portal associated with Petty Pool College.
Connecting a device via the Petty Pool College network.
Any electronic communication with a Petty Pool College Learner, member of Staff or contractor.
From any geographic location both on Campus and off Campus.

3. RESPONSIBILITIES

3.1 The reporting responsibilities for e-safety follow the same lines of responsibility as the College Safeguarding policy.

To report a concern:

- Make a written record of your concern, including the date, time and all relevant details of the person concerned, others involved and witnesses (if there are any)
- Contact your Designated Safeguarding Lead (DSL) or the Deputy (DDSL) who will inform you of the next actions to take.
- Complete a safeguarding event log on Databridge and including all necessary information and tag the relevant people into the entry.
- If it is an emergency and the learner is at risk of immediate serious harm, inform the police or social services immediately. Inform the DSL as soon as practicably possible.

To report a low-level concern or observation contact your DSL to discuss and they will decide if any escalation is required. All low-level concerns will be recorded and monitored within Databridge.

3.2 All Staff

- Are responsible for ensuring the safety of learners.
- MUST report any concerns or disclosures immediately to the Designated Safeguarding Lead (DSL)
- NEVER offer assurance of confidentiality everything discussed MUST be reported.
- MUST always keep to the terms and conditions of the ICT Acceptable Use Policy.
- MUST attend staff training on e-safety and always display a model example to learners.
- MUST actively promote through embedded good e-safety practice.

- MUST always communicate with learners professionally and in line with the college Communications Policy.
- WILL reinforce the importance of online safety when communicating with parents and carers. This includes making parents and carers aware of what we ask young people to do online (e.g., sites they need to visit or who they'll be interacting with online)

3.3 Learner

- MUST always keep to the terms and conditions of the ICT Acceptable Use Policy.
- MUST receive appropriate e-safety guidance as part of their programme of study.
- MUST Inform a member of staff where they are worried or concerned an e-safety incident has taken place involving them or another member of the college community.
- Learners MUST always act safely and responsibly when using the internet and/or mobile technology.

3.4 Safeguarding Champions

- MUST follow the safeguarding Reporting Procedure at all times.
- With management approval refer to appropriate additional support from external agencies.

3.5 Safeguarding Lead

- Leading the Safeguarding Committee
- Leading on e-safety meetings and any actions in line with KCSIE guidance 2023
- Ensuring delivery of staff development and training
- Recording incidents
- Reporting any developments and incidents to the Senior Management Team and Trustees.
- Liaising with the local authority and external agencies to promote e-safety within the College community.
- Take overall responsibility for the filtering and monitoring systems and processes in place at our college.

3.6 IT / MIS Department

- Ensure the Colleges IT infrastructure is secure and meets best practice recommendations.
- IT security incidents are recorded, investigated, and resolved within a reasonable timescale.

- MUST report any e-safety concerns or disclosures immediately to the (Designated Safeguarding Lead DSL)
- Any extension of this policy will require the express written permission of the SMT and Trustees

3.7 Principal

- Make sure that online safety training is included in staff safeguarding and child protection training.

3.8 Trustees

- Ensure that the college has appropriate filtering and monitoring systems in place and review their effectiveness. This includes:
    - Make sure that the leadership team and staff are aware of the provisions in place, and that they understand their expectations, roles and responsibilities around filtering and monitoring as part of safeguarding training.
    - Review the DfE's filtering and monitoring standards, and discussing with IT staff and service providers what needs to be done to support the school in meeting these standards.
    - Make sure the DSL has lead authority for safeguarding, including online safety and understanding the filtering and monitoring systems and processes in place.
    - Ensure all staff undergo safeguarding and child protection training, including online safety, and that such training is regularly updated and is in line with advice from the safeguarding partners.

4.0 MONITORING

4.1 The Petty Pool College activity monitor, log and report on learners and staff use of IT systems and IT network usage as part of the College's responsibility towards the 'safeguarding of young people and vulnerable adults' and Prevent duty for terrorist and extremist behaviour.

4.2 An attempt to interfere or avoid the monitoring or logging of any IT systems will be referred to the Colleges disciplinary process.

4.3 Where requested this information will be securely shared with appropriate local authorities and external support agencies.

5.0 CYBER SECURITY

5.1 Any breach of the Computer Misuse Act 1990 including all forms of hacking or acquiring / accessing someone else's digital identity is a criminal offence and will be referred to the colleges disciplinary procedure and sent to the police for investigation.

6.0 TRAINING

6.1 Learners

Learners will be provided with e-safety guidance by tutors and have access to e-safety information. Tutorial planning will include appropriate and relevant e- safety guidance for learners.
Issues associated with E-safety apply across the curriculum and learners should receive guidance on what precautions and safeguards are appropriate when making use of the internet and mobile technologies. Learners should also know what to do and who to talk to where they have concerns about inappropriate content, either where that material is directed to them, or where it is discovered as part of a random search. Within classes, learners will be encouraged to question the validity and reliability of materials researched, viewed or downloaded. They will also be encouraged to respect the copyright of other parties and to cite references properly.

6.2 For staff

Staff will receive an introductory session for digital learning/working systems and environments within the induction period. This introductory session will signpost the E-Safety Policy and provide an overview for academic staff. Formal agreement to the expectations and terms will be managed by the Human Resources Manager. Each member of staff must record the date of the training attended on their CPD calendar.
Any new or temporary users will also be asked to sign the college IT Acceptable Use Policy.

7.0 BEHAVIOUR

Use of any Petty Pool College IT equipment and systems is conditional to signing to say they have read the relevant College Policies including the e Safety and Social Media Policy and the IT Acceptable Use Policy. Communications by staff and learners should be courteous and respectful at all times whether offline or online. Any reported incident of bullying or harassment or other unacceptable conduct will be treated seriously in line with the relevant discipline policies.

8.0 CYBER BULLYING

8.1 Cyber bullying is a form of bullying. As it takes place online, it is not confined to college buildings or college hours. Cyber bullies can communicate their messages to a wide audience with speed and often remain anonymous or unidentifiable.

8.2 Cyber bullying includes bullying via:
Text message and messaging apps e.g., sending unwelcome texts or messages that are threatening or cause discomfort.
Picture/video-clips e.g., using mobile device cameras to bully someone, with images usually sent to other people or websites.
Phone call e.g., silent calls or abusive messages. The bully often disguises their number.
Email e.g., emailing upsetting messages, often using a different name for anonymity or using someone else's name to pin the blame on them.
Chat room e.g. sending upsetting responses to people when they are in a web-based chat room.
Instant Messaging (IM) e.g., sending unpleasant messages in real-time conversations on the internet.
Websites e.g., insulting blogs, personal websites, social networking sites and online personal polling sites.

8.3 Where conduct is found to be unacceptable, the College will deal with the matter internally and refer to relevant policies, for example, the Disciplinary Policy. Where conduct is considered illegal, the college will report the matter to the police.

9.0 SAFEGUARDING & PREVENT

9.1 Staff should beware of the Colleges responsibility of the Prevent Duty and Safeguarding of young people and adults at risk.

9.2 The following guidance must be adhered by all staff communicating online:
Staff must not post any personal views, beliefs, or opinions
Staff must challenge any personal views, beliefs or opinions posted by learners
Staff must report any personal view, belief or opinion posted by a learner which undermines British values. A member of staff with media training may post a counter argument to uphold the organisations position.
Any post considered to isolate or put a young person or vulnerable adult at risk should be referred to the Designated Safeguarding Lead for further investigation.
Any post considered to promote extreme views should be referred to the Designated Safeguarding Lead for further investigation.

10.0 ONLINE COMMUNICATION

10.1 Online communication must:

- Be concise
- Be engaging and use appropriate language
- Use decent-quality images whenever possible
- Use British English, correct spelling, and grammar
- Follow the appropriate style and brand guidelines

11.0 SOCIAL MEDIA

Use of Petty Pool College social media accounts

Only employees who have been authorised to use social media accounts through the College's social media approval process may access social media on the College network or create, maintain, or post on behalf of official College accounts.
The use of social media will only be approved where it is deemed to benefit learners and learning, is in the business interests of the College, and meets safeguarding and PREVENT duties.
The College has a number of official social media communications channels, which are part of the College infrastructure. These take priority in externally published documents and materials.
In the event of an incident or emergency involving Petty Pool College no content should be posted to any social media channels without the explicit permission of SMT

11.2 CREATING NEW SOCIAL MEDIA ACCOUNTS

New social media accounts that use an official logo or a Petty Pool College name must not be created unless approved by SMT.
In addition to this, all social media accounts must be always accessible by a second administrator. When an administrator leaves the College, their access to College social media accounts must be revoked, and the account either handed over to another administrator or closed.
The College will close down any "unofficial" social media sites using the Colleges logo, name or copyrighted materials, even if created by staff or students.

11.3 ONLINE PRIVACY AND PERSONAL INFORMATION

College employees must be aware of their social media presence, particularly when the social media account openly states that they work within the College.

Your social media presence on sites such as Facebook can contain a lot of personal information that you might not wish to share with your colleagues, employer or the general public.
Unless your privacy settings are restricted, your colleagues, employers and students may be able to access your personal information. Therefore, it is important to ensure that your privacy settings reflect the amount of information you want people to find out about you.
On Facebook in particular, there are many settings which can be altered to automatically restrict people's access to your profile; however, your cover image, name and profile pictures are able to be viewed by anyone with access to the site. Employees must ensure that their Facebook content and posts are restricted to people in their friends list.
It is recommended that other staff personal profiles are set to the maximum possible security settings. This means that only you and people in your friends and/or followers list will be able to see the updates you post.
Members of staff are responsible for managing their own social media presence and ensuring that their privacy settings are correct. Staff members are responsible for ensuring that their privacy settings are appropriate for the type of content they share on social media.

11.4 COLLEGE REPUTATION

College employees and learners are expected to respect the Colleges reputation when posting online.
Any information which may be consider damaging the Colleges reputation may result in disciplinary and/or legal action
Use of the Colleges Intellectual Property (IP) must be requested and approved by SMT. Any use of IP without permission may result in disciplinary and/or legal action.

11.5 ACCEPTING FRIENDS / FOLLOWERS

Employees of the Petty Pool College must maintain professional boundaries at all times, particularly when accepting or inviting 'friend' connections on personal social media accounts.
Employees must not passively or actively connect on social media with current or ex-students who are under the age of 18 or who have a vulnerability, adult students who they teach, support or could be deemed to give unfair advantage to, or any other persons deemed inappropriate by the Designated Safeguarding Lead.
People who studied within the College when they were under the age of 18 must not be added as connections by members of staff until five years after they have left the Petty Pool College.
Entering into such relationships may lead to abuse of an employee's position of trust and breach the standards of professional behaviour and conduct expected at the College. The College reserves the right to take

disciplinary action if employees are found to be in breach of this policy, with the potential of dismissal for serious breaches.
Acts of a criminal nature or any safeguarding concerns may be referred to the police, Local Safeguarding Adult and Children Board and/or the Independent Safeguarding Authority.
Exceptions to this rule can be made when the primary connection between an employee and a restricted person does not stem from them being a student of, or from interactions within, the College, and this has been declared to the Safeguarding Officer.
When the social media account uses a passive connection, such as the 'follow' action on Twitter and Instagram, employees must not 'follow' learners or ex-students under the age of 18. In the event that a student or ex-student under the age of 18 'follows' a College employee, the employee must be aware that the person may be able to access private information and images shared by the employee.
If an employee becomes aware of a student under 18 or a vulnerable adult who has 'followed' those, employees must block them.

11.6 USING SOCIAL MEDIA IN THE EMPLOYEE RECRUITMENT PROCESS

The College may view relevant social media websites and do a google search as part of the pre-employment process, these searches may include, but are not limited to, social media sites such as LinkedIn. Any information which relates to the applicants' protected characteristics under the Equality Act 2010 will not be used as part of the recruitment and selection process.

11.7 SOCIAL MEDIA APPROVAL PROCESS

All employees who want access to view, create or maintain social media accounts operated in the college must have read this policy and be approved as users by the relevant SMT member.

11.8 SOCIAL MEDIA IN TEACHING AND LEARNING

Social media can help in reaching learners to inform them of course related activities, events and news. Social media can be used to enhance a learner's experience through carefully planned use in teaching and learning, however social media platforms must not be the primary learning environment for learners.
Course content, collaborative working, group discussion and class level communication must be based within the agreed College learning and working environments.
Learners are not obliged to create social media accounts in order to access course materials and learners should not be disadvantaged by choosing not to participate within a social media platform.

12.0 COPYRIGHT

12.1 Staff and Students are responsible for ensuring they have the appropriate copyright licence for the use of any content or media being used.
All copyrighted material must be obtained from a legitimate licensed source.
The distribution of material which infringes copyright is a criminal offence and will be referred to the Colleges disciplinary process and/or the police for investigation.
The use of file sharing software including but not limited to Bit torrent is forbidden over the College network
The use of any website must be used within accordance of the website terms and conditions.
The downloading of YouTube videos for offline use is not permitted by the terms and conditions of the website.
Copyright guidance for learning resources is available from the MIS manager.

13.0 USE OF IMAGES AND VIDEO

Where the College has a "Lawful basis for processing" the use of images, or photographs, is popular in teaching and learning and should be encouraged. This will include images downloaded from the internet and images belonging to staff or learners.
Images & Videos of learners must be stored within approved College systems and must never been stored or sent to personal devices or accounts.
Our aim is to reinforce good practice as well as offer further information for all users on how to keep their personal information safe – e.g. there are particular risks where personal images are posted onto social networking sites.
No image/photograph can be copied, downloaded, shared or distributed online without permission from the owner of that image. Photographs of activities on the College premises should be considered carefully and have the consent of the Management Team before being published. Approved photographs should not include names of individuals.

14.0 A.I. (Artificial Intelligence)

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

College recognises that AI has many uses, including enhancing teaching and learning, and in helping to protect and safeguard pupils. However, AI may also have the potential to facilitate abuse (e.g., bullying and

grooming) and/or expose pupils to harmful content. For example, in the form of 'deepfakes', where AI is used to create images, audio or video hoaxes that look real.

College will treat any use of AI to access harmful content or bully pupils in line with this policy and our Behaviour policy.

Staff should be aware of the risks of using AI tools whilst they are still being developed and should carry out risk assessments for any new AI tool being used by the college.

14.0 FEEDBACK AND USEFUL INFORMATION

Petty Pool College welcomes all constructive feedback on this and any other college policy. If you would like further information on e-safety, or wish to send us your comments on our e-Safety Policy, then please contact the Assistant Principal, Data and Performance.
Useful Links for further Information:
Child Exploitation & Online Protection Centre
http://www.ceop.police.uk/
Internet Watch Foundation
https://www.iwf.org.uk/
Get Safe Online
https://www.getsafeonline.org/