PRESTON MUSLIM GIRLS HIGH SCHOOL

Education with Patience Modesty Gratitude Humility Sincerity

PUPIL ICT ACCESIBLE USE POLICY

Approved by:	Headteacher/Governing Board	**Date:** 17 December 2024
Last reviewed on:	November 2024	
Next review due by:	November 2026	

Document Control

Owner	Governors		
Date effective from	November 22	Date of next review	November 24
Review period	2 years	Version	22/1

Summary of changes in this version

Information
1st

Contents

Introduction

1. ICT in the 21st Century is seen as an essential resource to support learning and teaching, as well as playing an important role in the everyday lives of children, young people and adults. Consequently, schools need to build in the use of these technologies to arm our young people with the skills to access life-long learning and employment.
2. The school recognises the importance of information and communications technology (ICT) in education. The internet and other digital information and communication technologies are powerful tools, which can open up new opportunities for everyone.
3. Information Technology has the potential to enhance the quality of teaching and learning across the Curriculum. Using lCT in the classroom will help you cope with the future demand with a higher level of technological knowledge and awareness. This should help you become comfortable with the new technology and also can adapt to the rapid progress in this field.
4. Information and Communications Technology covers a wide range of resources including web-based and mobile learning. It is also important to recognise the constant and fast paced evolution of ICT within our society as a whole. Currently the internet technologies children and young people are using both inside and outside of the classroom include:
   - Websites
   - Learning Platforms and Virtual Learning Environments
   - E-mail and Instant Messaging
   - Chat Rooms and Social Networking
   - Blogs and Wikis
   - Podcasting
   - Video Broadcasting
   - Music Downloading
   - Gaming
   - Mobile/ Smart phones with text, video and/ or web functionality
   - Other mobile devices with web functionality
5. At PMGHS we understand the responsibility to educate our pupils on eSafety issues. teaching them the appropriate behaviours and critical thinking skills to enable them to remain both safe and legal when using the internet and related technologies, in and beyond the context of the classroom.
6. We have a range of Information and Learning Services that you will use during your time here. This is an easy-to-understand overview of the guidelines you need to be aware of, and comply with. This will ensure the effective running and security of the school's ICT services, and also protect you and your information.
7. This policy applies to all school computers and devices (including Wi-Fi) and also any mobile and tablet devices that you use in school.
8. Both this policy and the ELECTRONIC INFORMATION AND COMMUNICATIONS SYSTEMS POLICY (for all staff, governors, visitors and pupils) are inclusive of both fixed and mobile internet; technologies provided by the school (such as PCs, laptops, personal digital assistants (PDAs), tablets, webcams, whiteboards, voting systems, digital video equipment, etc); and technologies owned by pupils and staff, but brought onto school premises (such as laptops, mobile phones, camera phones, PDAs and portable media players, etc).

Aims

9. To provide you with a set of rules you will be expected to adhere to when using the school's ICT equipment.

10. To inform you of what you can and cannot use the school's ICT equipment for.
11. To provide guidance on how to correctly use the school's ICT equipment to save and store your work.
12. To provide information on how to effectively manage your individual user account and set your password.
13. To ensure that you use the internet safely and responsibly.
14. To promote e-safety throughout the school and provide advice on how to deal with matters such as cyber bullying.
15. To support the mission, vision and values of PMGHS.

Who is responsible for this policy?

16. The Governors have overall responsibility for the effective operation of this policy and for ensuring compliance with the relevant statutory or Trust framework. The Governors have delegated day-to-day responsibility for operating the policy to the Headteacher and Network Manager of the school.
17. The Local Governing Body and Senior Leadership Team at the school have a specific responsibility to ensure the fair application of this policy and all members of staff are responsible for supporting colleagues and ensuring its success.

The Data Protection Act in Schools (GDPR)

18. Any organisation that handles personal information must comply with the Data Protection Act 2018 (as amended in accordance with GDPR). However, some organisations have greater data protection risks than others, and this is particularly the case in schools. They must handle personal data about staff and students securely and confidentially, which requires them to implement robust systems and management strategies.
19. You must know how to help your school fulfil these data protection requirements, so everyone's personal information is acquired and held securely at all times. This guide will help you understand what duties you should fulfil to uphold data protection in your school.

Personal Responsibility

20. As a representative of PMGHS, you will accept personal responsibility for reporting any misuse of the network to a staff member. Misuse may come in many forms, but it is commonly viewed as any message(s) sent or received that indicate or suggest pornography, unethical or illegal requests, racism, sexism, inappropriate language, any use which may be likely to cause offence and attempts to disrupt or hack into the computer network.

Acceptable Use

21. The use of ICT must be in support of education and research in accordance with the educational goals and objectives of PMGHS. Students are personally responsible for this provision at all times when using any ICT resource.
22. Transmission of any material in violation of any United Kingdom or other national laws is prohibited. This includes, but is not limited to, copyrighted material, threatening or obscene material or material protected by trade laws.
23. Use for commercial activities by for-profit organisations or personal enterprise is generally not acceptable.

Privileges

24. The use of the ICT is a privilege and inappropriate use can result in that privilege being withdrawn. Students will participate in a discussion with a member of staff as to proper behaviour and use of the facilities. Staff will rule upon inappropriate use and may deny, revoke or suspend usage.

Network Etiquette and Privacy

25. You are expected to abide by the generally accepted rules of network etiquette. These rules include, but are not limited to, the following:
    25.1. **BE POLITE.** Never send or encourage others to send abusive messages. Respect the rights and beliefs of others
    25.2. **USE APPROPRIATE LANGUAGE.** Remember that you are a representative of the Trust on a global public system. Never swear, use vulgarities or any other inappropriate language. Illegal activities of any kind are strictly forbidden.
    25.3. **PRIVACY**. Do not reveal any personal information to anyone, especially the home address or personal telephone of yourself or any other students.
    25.4. **PASSWORD.** Do not reveal your password to anyone. If you think someone has obtained your password, contact a member of ICT Support immediately.
    25.5. **ELECTRONIC MAIL**. Electronic mail (e-mail) is not guaranteed to be private. Messages relating to, or in support of, illegal activities may be reported to appropriate authorities.
    25.6. **REFERENCE WORK.** Cite references for any facts that you present. Do not copy other people's work and imply that it is your own (i.e plagiarism). Plagiarism leads to formal action, up to and including, withdrawal from examination and qualifications.
    25.7. **DISRUPTIONS**. Do not use the network in any way that would disrupt use of the services by others.

Services

26. PMGHS makes no warranties of any kind whether expressed or implied, for the network service it is providing. PMGHS will not be responsible for any damages suffered whilst on this system. These damages include loss of data as a result of delays, non-deliveries, mis-deliveries or service interruptions caused by the system or elements of the system, errors or omissions. Use of any information obtained via the network or other information systems is at your own risk. PMGHS specifically denies any responsibility for the accuracy of information obtained via its Internet services.

Security

27. If you identify a security problem, notify a member of ICT Support at once. Never demonstrate the problem to another student. All use of the system must be under your own username and password. Remember to keep your password to yourself. Do not share it with friends. Anyone caught disclosing passwords may have their access denied and may be subject to disciplinary action. Any user identified as a security risk may be denied access to the system and be subject to disciplinary action.

Vandalism

28. Vandalism is defined as any malicious attempt to harm or destroy any equipment or data of another user or of any other networks that are connected to the system. This includes, but is not limited to, the uploading or creation of computer viruses, the wilful damage of computer hardware, whether connected to the network or not, the deletion of data from its place of storage.

Online Ordering systems

29. It is strictly forbidden for students to use the Internet for ordering goods or services regardless of their nature. In addition, it is also forbidden for students to subscribe to any newsletter, catalogue or other form of correspondence via the Internet, regardless of its nature.

Electronic Mail

30. Electronic mail (email) is provided by PMGHS, the use of Internet based email systems is forbidden. The sending or receiving of any email, which contains any inappropriate material, is strictly forbidden. This material includes, but is not limited to, pornography, unethical or illegal requests, racism, sexism, inappropriate language, any use which may be likely to cause offence. Disciplinary action will be taken in all cases. It is also forbidden to send large volume emails (spamming).

Non-Educational Online Activity

31. You are not permitted to access non educational games, media (e.g. YouTube) or chat services available online.

Internet Search Engines

32. You are required to use Internet search engines responsibly. If students are found to be searching for material unsuitable and in breach of this policy they will face disciplinary action. Students are strictly forbidden from removing safety filters from Internet Search engines in order to access unsuitable material. This includes but is not limited to the removal of the SafeSearch feature.

Executable, Music and Video Files

33. You are strictly forbidden from introducing executable files (e.g. '.exe, .cmd, .bat, .bin') to the network as these can is some cases contain harmful viruses. This includes but is not limited to copying such files onto shared network drives, saving them on your Home Area (H:\) and running them from your USB memory stick.
34. You are strictly forbidden from introducing music and video files (e.g. '.mp3, .mp4, .mpeg, .wav, .avi'). These files in many cases are copyrighted and the copying onto shared network drives or storing on your Home Drive (H:\) may breach their copyright.
35. You are strictly forbidden from downloading executable, music and video files when using the school's internet provision.

Accessing Remote Systems

36. you are only permitted to access remote systems authorised by PMGHS.

Pupil accounts: setting your password

37. When joining the school you are allocated an account which you take responsibility for. This account enables you to access the school provided systems (e.g., Microsoft Teams) and you are responsible for all the activity that takes place under your username. Ordinarily passwords are provided by the school, however if you are asked to set a password for your account you should:
    - use a combination of letters, numbers and symbols;
    - try using a memorable saying or phrase;
    - not tell anyone your password and never write it down.
38. If you are worried someone has guessed your account password, you will need to immediately inform a member of staff.

Pupil accounts: saving your work

39. Your personal space on the school ICT network is known as OneDrive. You should save your work to the school OneDrive unless advised otherwise by a member of staff.

40. Do not save to the C: drive on school computers as this is not backed up.
41. You must not use external media (e.g. USB memory and external hard disks) as your primary storage repository as it is not possible to recover lost or corrupted files. Students are advised to save all files OneDrive where it is routinely backed up and easily accessed both onsite and remotely. Students are advised to regularly save amendments to their files to minimise data loss if their service is interrupted.
42. If you do save to a USB memory stick, make sure that you know which the most recent version is and also keep a backup copy.

Pupil accounts: Microsoft Teams

43. The user login account you are provided with allows you to access school provided services such as Microsoft Teams. You are expected to use this and other services in a responsible manner, and do so in accordance with the following guidelines:
    - Do not attempt to access accounts that belong to other pupils or school staff;
    - Do not use accounts that belong to others unless permission has been granted;
    - Do not open or forward any information or attachment, or other communication from an unrecognised source or that you suspect may contain inappropriate material or viruses report the item to a member of staff;
    - Do not send, forward, share, print or transmit - in any form - any offensive, obscene, violent, or dangerous material;
    - Do not send, forward, or share chain letter emails, jokes, spam etc;
    - Do not reveal any personal information about yourself or anyone else, especially home addresses, personal telephone numbers, usernames, or passwords;
    - Use appropriate language - what you say and do can be viewed by others;
    - Consider the file size of an attachment, files exceeding 25MB in size are generally considered to be excessively large and you should consider using other methods to transfer such files (speak to a member of staff to find out how to do this) (if allowed).
    - your behaviour in the virtual classroom should mirror that in the physical classroom.
44. If you are concerned about any communication you have received, you should contact a member of staff immediately.

Use of the internet

45. A web-filtering system is in place at the school. Although internet usage is supervised and filtered within the school, it is impossible to guarantee that all potentially harmful material is filtered. Some pupils may find ways to access material that is inaccurate, defamatory, illegal or potentially offensive to some people. If you come across any inappropriate website or content whilst using the ICT equipment, you must report it to a member of staff immediately.
46. The use of the internet is a privilege and inappropriate use will result in sanctions being applied by the school.
47. All internet access is logged and monitored. Use of the internet should be in accordance with the following guidelines. You must:
    - not upload any files to social media sites; this includes images or videos that are taken on school premises;
    - only access suitable material – the internet is not to be used to download, send, print, display or transmit material that would cause offence or break the law (this includes accessing sites meant for adults of 18 years or older such as pornographic or gambling sites);
    - not access internet chat sites - you could be placing yourself at risk;

- never give or enter your personal information on a website, especially your home address,
- your mobile number or passwords;
- not access online gaming sites - your use of the internet is for educational purposes only;
- not download or install licenced or unlicenced software from the internet,
- not use the internet to order goods or services from online shopping or auction sites;
- not subscribe to any newsletter, catalogue or other form of correspondence via the internet;
- not download any unlicensed material such as music, videos, TV programmes, games, and PDF files - this is considered illegal and therefore not permitted.

Use of ICT equipment

48. You have a responsibility towards the care of any school ICT equipment.
49. You must keep all liquids and food away from any ICT equipment.
50. Downloading and installing software packages, whether licenced or unlicenced, on school-owned equipment is not permitted.
51. You must not:
    - allow anyone to use your device when you are logged in;
    - use another user's device without their permission;
    - copy or distribute licenced software for installation on other ICT equipment;
    - deliberately port scan or use port scanning software;
    - use peer to peer file sharing software to download or upload obscene, copyrighted, or illegal material;
    - connect or attempt to connect to ICT systems without permission;
    - run server operating systems or services without permission;
    - connect any form of network device (i.e. routers, wireless access points, switches, or hubs) to the ICT network;
    - deliberately or unintentionally cause the interruption of any school service or another user's data or system e.g. by virus infection;
    - save personal media images, sound, and videos on the file server network.
52. You should report all faults or damage to school-owned equipment to a member of staff.
53. If the school has loaned you any ICT equipment to use at home, you must follow the same set of rules within this policy.
54. Vandalism to ICT equipment will result in sanctions and parents will be asked to make payments for any malicious damage to the ICT equipment. Vandalism is defined as any malicious attempt to harm or destroy data of another user and deliberately decorate or damage ICT equipment.
55. Incidents of accidental damage will be dealt with on a case-by-case basis by the school. Social networking sites
56. You are not permitted to access social networking sites such as Facebook, Twitter and Instagram on school equipment (either in the classroom or at home, via a loaned laptop).
57. You are not permitted to have staff at the school as contacts on social networking sites.

Loss of data

58. The school will not be responsible for any loss of data if this is caused as a result of your negligence, errors or omissions.

Online bullying

59. The school will not tolerate any form of bullying including electronic or online bullying. Sending or publishing offensive or untrue messages or imagery that could intimidate, harm or humiliate other pupils and their families is forbidden and could be regarded as breaking the law.
60. The school reserves the right to monitor all internet and email activity within the bounds of current legislation in order to keep the internet safe for all at the school and to protect from online bullies.
61. Any instances of bullying will be taken very seriously. As with any other form, cyber or online bullying will be investigated fully and will result in disciplinary action.

Hacking

37. Any type of hacking (an attempt to gain access to folders, databases, or other materials on the network to which you are not entitled) is considered to be an extremely serious offence.
62. Similarly, physical interference with another user's computer is not permitted.

Copyright

63. You must not copy or store files, documents, music, video or any other material where copyright restrictions exist, unless permission by the copyright holder has been given. Using copyright material without permission is an offence.

Monitoring

64. Authorised staff may monitor, intercept, access, inspect, record and disclose telephone calls, e-mails, instant messaging, internet/intranet use and any other electronic communications (data, voice or image) involving its employees or contractors, without consent, to the extent permitted by law. This may be to confirm or obtain School business related information; to confirm or investigate compliance with School policies, standards and procedures; to ensure the effective operation of School ICT; for quality control or training purposes; to comply with a Subject Access Request under the Data Protection Act 1998, or to prevent or detect crime.
65. All monitoring, surveillance or investigative activities are conducted by ICT authorised staff and comply with the Data Protection Act 1998, the Human Rights Act 1998, the Regulation of Investigatory Powers Act 2000 (RIPA) and the Lawful Business Practice Regulations 2000.
66. Please note that personal communications using School ICT may be unavoidably included in any business communications that are monitored, intercepted and/or recorded.

Sanctions

67. The following sanctions may be applied if these rules are not followed:
    - Restricted access to the internet or computer use;
    - Additional disciplinary action may be taken in line with the Behaviour Policy;
    - When applicable, police or the Local Authority may be involved.
68. Depending on the circumstances, your parent(s)/carer(s) may be informed of any breaches of this policy.

Appendix A:

PRESTON MUSLIM GIRLS HIGH SCHOOL

Education with Patience Modesty Gratitude Humility Sincerity

Ref

DATE

Dear Parents and Carers

ICT Code of Conduct

Assalamualaikum, I hope and pray this letter finds you in the best of health and Imaan.

As part of your daughter's curriculum and the development of ICT skills, we provide a range of IT facilities including access to the Internet. We believe that the use of the internet through the web is worthwhile and is an essential skill for children as they grow up in the modern world.

Please read the attached ICT Code of Conduct with your daughter.

- Pupils are required to sign that they agree to abide by the Code of Conduct
- Parents are required to indicate their consent to their daughter accessing the Internet through the school's ICT facilities

Please note that your daughter will not be able to use the school's ICT facilities until this form has been returned.

Although there are genuine concerns about pupils having access to undesirable materials we take positive steps to deal with this risk in school. Our school's internet access is strongly filtered with a comprehensive system that restricts access to inappropriate materials.

Whilst every endeavour is made to ensure that suitable restrictions are placed on children accessing inappropriate material, the school cannot be held responsible for the nature or content of materials accessed through the internet. The school will not be liable for any damages arising from your daughter's use of the school's internet facilities.

Please note that pupils may be held liable for any damage willfully caused to the school's ICT facilities.

We advise you to read the School's ICT Policy which can be found together with other school policies on the School's website.

Yours sincerely

ICT CODE OF CONDUCT

The computer system is owned by the school and is made available to pupils to further their education and to staff to enhance their professional activities including teaching, research, administration and management. The school has an ICT Policy and ICT Code of Conduct to help protect all parties - the pupils, the staff and the school.

- Access should only be made via the authorised account and password that should not be made available to any other person
- Users will only access their own files
- Users will not access or delete other people's files
- Users will only make contact with people they know or have been instructed to by their teacher
- Users will not give out personal information including their address, phone number, financial information, or arrange to meet someone in person
- The security of the ICT system must not be compromised
- Pupils must only access sites and materials that are appropriate to work in school Users will not access inappropriate websites using the school's ICT facilities
- Users are responsible for all emails sent and for contacts made that may result in email being received
- Users must be mindful of the costs incurred for printing and use this sparingly.
- The same professional levels of language and content should be applied in emails as for letters or other media, particularly as emails are often forwarded
- E mails will not contain abusive or inappropriate language or material
- Posting anonymous messages and forwarding chain letters is forbidden.
- Copyright of materials and intellectual property rights must be respected
- Use for personal financial gain, gambling, political purposes, or advertising is forbidden the use of public chat rooms is not allowed
- Users will be expected to report anything they see that they feel unhappy about or if they receive a message they do not like
- Users are not permitted to store personal photographs, music, or video files on the school network
- Users will not use proxy websites to access banned sites on the school's network
- Use of social networking sites is not allowed, and such sites are blocked
- Communication between staff and pupils should only be through the school's email address
- Use of social networking sites is not allowed, and such sites are blocked
- Communication between staff and pupils should only be through the school's email address

All users are advised that they should not deliberately seek out inappropriate/offensive materials on the Internet and that they may be subject to the school's disciplinary procedures should they do so.

It is expected that all staff and pupils will abide by this policy. Failure to do so will result in disciplinary action being taken.

This is currently being reviewed by the school, any updated versions to this policy will be provided once it has been ratified by the governors.

ICT CODE OF CONDUCT

PUPIL AND PARENT AGREEMENT

PUPIL AGREEMENT
I have read and understand the school's ICT Code of Conduct and I agree to abide by its rules.

Name of Pupil:	**Registration Form:**
Pupil's signature:	**Date:**

PARENT/CARER CONSENT FOR INTERNET ACCESS

I have read and understand the school's ICT Code of Conduct and give permission for my daughter to access the Internet.
I understand that the school will take all reasonable precautions to ensure pupils cannot access inappropriate materials. I understand that the school cannot be held responsible for the nature or content of materials accessed through the Internet. I agree that the school is not liable for any damages arising from the use of the Internet facilities

Please note that your daughter will not be able to access the school's ICT facilities until this form has been returned.

Name of Parent/Carer:	
Parent/Carer's signature:	**Date:**