PRESTON MUSLIM GIRLS HIGH SCHOOL

Education with Patience Modesty Gratitude Humility Sincerity

ICT ACCEPTABLE USE POLICY

RATIFIED BY THE FULL GB – October 2017

REVIEW DATE – September 2018

01772 651906 | www.pmghs.com | info@pmghs.com
Quwwatul Education Centre, Peel Hall Street, Preston, PR1 6QQ

Introduction

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 in order to arm our young people with the skills to access life-long learning and employment.

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

Whilst exciting and beneficial both in and out of the context of education, much ICT, particularly web-based resources, are not consistently policed. All users need to be aware of the range of risks associated with the use of these Internet technologies.

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.

Schools hold personal data on learners, staff and other people to help them conduct their day-to-day activities. Some of this information is sensitive and could be used by another person or criminal organisation to cause harm or distress to an individual. The loss of sensitive information can result in media coverage, and potentially damage the reputation of the school. This can make it more difficult for your school to use technology to benefit learners.

Everybody in the school has a shared responsibility to secure any sensitive information used in their day to day professional duties and even staff not directly involved in data handling should be made aware of the risks and threats and how to minimise them.

Both this policy and the Acceptable Use Agreement (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).

Monitoring

ICT 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.

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.
Please note that personal communications using School ICT may be unavoidably included in any business communications that are monitored, intercepted and/or recorded.

Breaches

A breach or suspected breach of policy by a School employee, contractor or pupil may result in the temporary or permanent withdrawal of School ICT hardware, software or services from the offending individual.

Any policy breach is grounds for disciplinary action in accordance with the School Disciplinary Procedure.

Policy breaches may also lead to criminal or civil proceedings.

The Information Commissioner's Office (ICO) new powers to issue monetary penalties came into force on 6 April 2010, allowing the ICO's to serve notices requiring organisations to pay up to £500,000 for serious breaches of the Data Protection Act.
The data protection powers of the Information Commissioner's Office are to:

- Conduct assessments to check organisations are complying with the Act;
- Serve information notices requiring organisations to provide the Information Commissioner's Office with specified information within a certain time period;
- Serve enforcement notices and 'stop now' orders where there has been a breach of the Act, requiring organisations to take (or refrain from taking) specified steps in order to ensure they comply with the law;
- Prosecute those who commit criminal offences under the Act;
- Conduct audits to assess whether organisations processing of personal data follows good practice,
- Report to Parliament on data protection issues of concern

Incident Reporting

Any security breaches or attempts, loss of equipment and any unauthorised use or suspected misuse of ICT must be immediately reported to the Network Manager or eSafety Co-ordinator. Additionally, all security breaches, lost/stolen equipment or data (including remote access), virus notifications, unsolicited emails, misuse or unauthorised use of ICT and all other policy non-compliance must be reported to your ICT Coordinator.

Acceptable Computer and Internet use statement for Staff and Students

Acceptable use policy – Students

The following letter is sent for signature by Parent/Guardian of students when they join the school.
Dear Parent(s) / (Carers)

USE OF THE INTERNET AND SCHOOL ICT EQUIPMENT

As part of our I.C.T. programme, we offer student's access to the Internet at school. To gain access, all students must obtain parental permission and return the slip below.

Access to the Internet is available throughout the school. It enables students to explore thousands of libraries, databases and information sources. Although we use a filtered service provided by Abzorb/Virgin and E Business, some material may be accessible that is inappropriate for school use.

Whilst our aim for Internet use is to further educational goals and objectives, students may find ways to access other materials as well. We believe that the benefits to students from access to the Internet outweigh the disadvantages. During lesson time teachers will guide students towards specific materials. Beyond lesson time, students must agree to access only those sites that are appropriate for their curricular studies. Parents share the responsibility for such guidance as with any other form of media, such as films, videos, television, magazines, etc., where inappropriate material can be found.

Please read the Code of Conduct for Internet Use and, if you agree to your daughter having access to the Internet, sign the slip below and return it to school. Failure to return this pro forma fully completed will mean access to the Internet and school network will not be granted.

Yours sincerely
ICT Co-ordinator and Head of Department

To: Ebrahim Nakuda, Network Support, PMGHS

COMPUTER & INTERNET PERMISSION FORM

STUDENT'S FIRST NAME:	
STUDENT'S SURNAME:	
STUDENT'S DATE OF BIRTH:	
STUDENT'S TUTOR GROUP:	YEAR GROUP:
PARENT/CARER SIGNATURE	