SCHOOL OPERATING POLICY

Kelvin Hall

ICT ACCEPTABLE USE

Internet and e-mail acceptable use policy for Pupils & Staff of Kelvin Hall School: A Specialist Science College

Scope

This document provides the acceptable standards for use of the internet and e-mail by all Kelvin Hall students & staff. It applies to all pupils and all school staff, whether employed by the School or working for the school through 3rd party agencies.

Responsibilities

Governing Body/Headteacher Responsibilities

It is the responsibility of the Governing Body to both adopt and review this policy on an annual basis and to advise the Headteacher of any required changes.

It is the responsibility of the Headteacher to publicise and make this policy available to all current and future school students & staff, and to ensure that the standards within it are both monitored and enforced and to advise the Governing Body of any serious breaches of the policy.

It is the responsibility of both the Headteacher and the Governing Body to take corrective and disciplinary measures as are necessary when a breach of this standard occurs and to contact and co-operate with police and other law enforcement agencies where a breach of these standards constitutes a criminal act.

All School Staff & Student Responsibilities

Students and staff must adhere to these standards in following circumstances:

- When working on schools premises
- When using equipment and utilities (hardware, software or mail and internet access) provided by the School or the LA at home or other locations

The standards apply regardless of whether access occurs during or outside of contracted work hours.

Students & staff must alert the Headteacher or a relevant senior member of staff where breach of these standards is suspected or known to have occurred. Failure to do so is also a breach of these standards.

E-mail Use

E-mail is provided for school business use and for educational and learning purposes, it is not a perquisite or a means of entertainment. Content of e-mails should be substantially related to school business or educational matters. E-mail should never be sent, forwarded or replied to where the content is Adult, Explicitly offensive or otherwise inappropriate as specified in table 1.1 below.

Table 1.1 Inappropriate email content definitions.

Abusive	**Bullying**	**Defamatory**
Disruptive	**Harmful to school morale**	**Harassing**
Insulting	**Intolerant**	**Obscene**
Offensive	**Politically biased**	**Sexual innuendo**
Violent	**Threatening**	**Racist**
Criminal or inciting criminal act(s)		
Prohibited material will include any material which may be construed as offensive on the grounds of gender, race, ethnic origin, disability, sexuality, religion, physical characteristics for trade union membership/office or any combination thereof.		

Internet Use

Access to the Internet is similarly provided for school business use and for educational and learning purposes. It is not a means of entertainment.

Sites visited should, be related to school matters.

Sites must not be accessed which contain inappropriate material as defined in table

Table 1.2 Inappropriate web content definitions.

Adult or explicit (including photo searches for such material)	Incitement (e.g. race hate or supremacist ideologies)	Chat rooms or Instant Messaging
Personal ads or dating	Criminal/Terrorist Skills or resources	Newsgroups & Forums
Downloads of ring-tones, screensavers and games	Internet based Peer to Peer networks e.g. Napster, etc.	Downloads of freeware, shareware or evaluation packages (except by authorised persons designated by the Headteacher and in compliance with copyright law)
Hacking, virus writing or password cracking	Illegal Drugs	Tasteless and offensive content such as, jokes, pictures or profanity
Gambling	Depiction or advocation of violence, or the use of weapons	Purchasing of goods or services (except by authorised persons designated by the school)
Intolerance toward religious beliefs and practices		Accessing data that does not have the owner’s permission to access

Good Practice for Students & Staff

- Be extremely cautious about revealing any personal details, and never reveal home address or telephone number in e-mails to those you don't know.
- Do not to use other people's user identities (user names) or passwords, even with their permission
- Do not allow others to use your username or password (on any system)
- Do not physically misuse any piece of ICT equipment
- If planning any activity (e.g. research into terrorism for a legitimate project) that might risk breaking this policy, students should ensure that at least one teacher of a relevant subject knows what is planned and has given advice.
- To report any breach (deliberate or accidental) of this policy to a Senior Member of Staff immediately - even if someone else breaches the policy, as it may affect younger students or visitors at a later time.
- Do not change or override security or access settings

Personal Use of the school's Internet and E-mail Provision

The sending of e-mails that are wholly or substantially unrelated to the school's business, or educational matters should be restricted to out of school hours and designated breaks.

Access to Internet web sites that are unrelated to the school's business, or educational matters should be restricted to out of School hours and designated breaks.

Personal use of both e-mail and the Internet must not breach any of the definitions of inappropriate use as defined in this document.

Conducting Financial Activities on the Internet

While this policy does not specifically ban the use of the Internet for conducting personal financial transactions e.g. E-banking, we warn against it. Residual information from such activities can be left on your computer hard drive and could subsequently be accessed by others. Neither the School nor the LA accept any liability for any resulting loss or damage.

Consequences of Breaching the Standards Laid out in this Policy

The use of e-mail to send, view or store other inappropriate content (as defined in table 1.1) or provision of an e-mail address to a 3rd party with the intention of receiving inappropriate content will constitute misconduct or gross misconduct.

Deliberate access to inappropriate web content (as defined in table 1.2) may constitute misconduct or gross misconduct.

Deliberate and repeated access to such material will constitute gross misconduct. The use of e-mail or the Internet for the preparation, commission or abetting of a criminal act will constitute gross misconduct.

Guidance on the use of Social Networking sites (e.g. Facebook, My Space) on staff's personal computers

Do not use such sites to have any contact with students.

- These sites are unregulated
- Examples of difficulties they can cause teachers/other staff include
- Content being downloaded, amended to give it a spin and then "published". Most students are more adept at both using and misusing ICT than many of us
- Contact being used as evidence of "grooming"
- It makes no difference who initiated the contact
- "My Classes" is a regulated and transparent site for appropriate contact with students about homework, coursework etc. ICT Technicians can help you to set up a blog on "My Classes".

Be very mindful of personal information you make available on such sites

- Any information you place on such sites is in the public domain
- Your name may be sufficient for you to be identified as a teacher/other staff at Kelvin Hall. A picture will be conclusive.
- You must be certain that any personal information divulged will not compromise your professional status as a teacher or as a member of staff at the school. Some students and parents will exploit any signs of "weakness" you make available to them.
- You must be aware that you can harm the public image of the school without mentioning it by name. Your status as an employee at the school will be sufficient.

You should not publish any information/pictures about the school, or which could be linked to the school.

- Under the school's Disciplinary Procedures "Actions which could damage the public image of the school" could constitute gross misconduct.

Monitoring and Reporting

The school and the LA monitor the use of the Internet and e-mail.

Annual Review to Statement

The policy of ICT will be reviewed in accordance with the school improvement plan in consultation with staff

ICT Acceptable Use - Additions

Harmful Programs

Care must be must be taken to ensure any files which are put onto the school network are free from harmful (malicious) programs (such as viruses). This includes files which are put on using:

- Removable media (e.g. USB sticks, CDs or DVDs)
- Cloud storage (e.g. Google drive, Dropbox or OneDrive)
- Personal electronic devices (e.g. mobile phones, tablets, laptops, cameras and music players)

If you are unsure about any files ask an ICT technician to check them. This also applies to any files attached to an email.

Staff must not save files to the 'C;' drive of any computer. This is the hard drive attached to the computer and is not easily checked for malicious programs.

Applications must not be installed onto any electronic device (e.g. PCs and iPads) without direct permission from a member of staff.