IT Services

IT Acceptable Use & E-Safety Policy

1. Background

1.1 The College recognises the opportunities that technology brings to teaching, learning, assessment and research, giving users the opportunities to create, collaborate and explore in a digital world, using multiple devices from multiple locations.

1.2 College IT facilities and services are provided for bona fide College activities, for staff, students and approved visitors to the College.

1.3 Use of the College's IT & Communications systems and services is accessed through acceptance of the IT Acceptable Use & e-Safety Policy.

2. Purpose

2.1 The purpose of this policy is to protect and safeguard all users as well as to promote positive online behaviours. It also aims to reduce the risk of disciplinary or legal action by making users aware of the legislative and regulatory framework within which the ICT systems should be used.

2.2 We aim to equip students with the skills and knowledge they need to use technology safely and responsibly and to manage the risks of:

- Using the internet excessively/obsessively
- Physical danger of sexual or physical abuse
- Inappropriate, antisocial or illegal behaviour
- Exposure to inappropriate materials/groups (e.g. extremist organisations)
- Breaching legal obligations, including copyright
- Financial loss

3. Responsibilities

3.1 e-Safety is a whole College responsibility. The Managing Director, Professional Careers Academy will undertake the roll of e-Safety Coordinator; to promote e-Safety policies and systems for developing and maintaining a safe ICT learning environment.

3.2 The e-Safety Coordinator will:

- Oversee all areas of digital safeguarding at Highbury College.

- Act as a key point of contact on all e-safety issues
- Establish an e-safe culture by raising awareness and understanding of e-safety to all stakeholders, including parents and carers
- Embed e-safety in staff training, continuing professional development and across the curriculum and learning activities
- Maintain an e-safety incident log and report quarterly to the College Health & Safety Committee.
- Understand the relevant legislation
- Liaise with other agencies as appropriate
- Review and update e-safety policies and procedures

3.3 All teaching staff must promote the importance of e-Safety to students and seek opportunities to embed e-Safety in the curriculum. Updated April 2016 Approved – Operations Group April 2016

4. Policy

4.1 All users must take responsibility for their own use of information communication technology, ensuring that they use technology safely, responsibly and legally.

4.2 All users must be active participants in e-safety education, taking responsibility for their awareness of the opportunities and risks posed.

4.3 No communication device, whether College provided or personally owned, may be used for bullying or harassment of others in any form including through social media. This includes the creation or transmission of:

4.3.1 Any offensive, obscene or indecent images, data or other material

4.3.2 Material with intent to cause annoyance, inconvenience or needless anxiety;

4.3.3 Material which harasses, upsets or embarrasses a third party;

4.3.4 Material which promotes discrimination on the basis of race, sex, religion or belief, disability, age or sexual orientation.

4.4 The network and all associated devices must not be used for illegal activity in any form. This includes:

4.4.1 The creation, dissemination, storage and display of materials that promote terrorism or extremist ideologies.

4.4.2 The creation, dissemination, storage and display of indecent images of children.

4.4.3 The creation, dissemination, storage and display of hate literature.

4.4.4 The downloading, storage and disseminating of copyrighted materials, including software and all forms of electronic data, without the permission of the holder of the copyright or in transgression of the terms of the licence held by the College

4.4.5 The buying or selling of stolen goods.

4.5 No applications or services accessed by users may be used to bring the College, or its members, into disrepute.

4.6 All users have a responsibility to report any known misuses of technology, including the unacceptable behaviours of others, to the IT Services Department

4.7 All users have a duty to respect the technical safeguards, which are in place. Any attempt to breach technical safeguards, conceal network identities or gain unauthorised access to systems will result in disciplinary action. All users have a duty to report failings in technical safeguards, which may become apparent when using the systems and services.

4.8 All users have a duty to protect, and are not permitted to share their passwords and personal network logins. Users should lock or log off from their workstations when leaving them unattended. Any attempts to access, corrupt or destroy other users' data, or compromise privacy of others in any way, will result in disciplinary action. Updated April 2016 Approved – Operations Group April 2016

4.9 All users should use network resources responsibly. Wasting staff effort or network resources, or using the resources in such a way so as to diminish the service for other network users is unacceptable.

4.10 All users should be mindful of using the Internet and should not download or install any software or data which may not be licensed (see Software Policy) or contains viruses and spyware unless authorised to do so by the Head of Technology & Innovation.

4.11 Users are encouraged to bring their own devices (BYOD) and connect to College's wireless network; however they will ensure that these devices have the relevant updates and virus definitions. Use of these devices remains subject to this policy. Users must also ensure that the devices are electrically sound. Users who fail to have up to date antivirus or operating system updates may have their device blocked from the network.

4.12 Staff and Students using social networking sites (e.g. Facebook/Twitter), at any time or place, should do so with due consideration and care for fellow Staff and Students. The posting on social networking sites of any comments which may reasonably be considered to be offensive about Highbury College staff or students or the College as a whole will be considered to be a breach of this policy. Students may not use social networking sites in lessons unless permission is given by the teacher to do so.

4.13 Staff should not store private College information (for example confidential business information or personal data that is covered by the Data Protection Act) on portable computers or portable storage media without encryption.

5. Privacy & Monitoring

5.1 All users should understand that network activity and online communications are monitored, including personal and private communications made via the College network. This also includes the College's telephony systems. Any personal information collected during this monitoring is managed in accordance with the Data Protection Act. Reasons for such monitoring include the need to:

5.1.1 Establish the existence of facts (e.g. to provide evidence of commercial transactions in cases of disputes);

5.1.2 Investigate or detect unauthorised use of the College's telecommunications systems and ensure compliance with this policy or other College policies;

5.1.3 Ensure the operational effectiveness of services (e.g. to detect viruses or other threats to the systems);

5.1.4 Prevent a breach of the law or investigate a suspected breach of the law, the College's policies and contracts;

5.1.5 Monitor standards and ensure effective quality control.

5.2 Approval to access a user's data or personal areas may only be granted by IT Services after approval from the Principal & Chief Executive.

6. Violations and Responsibilities

6.1 All users should be aware that in certain circumstances where unacceptable use is suspected one of the following actions might be enforced:

- User's network account may be suspended.

- Enhanced monitoring and procedures may come into action (Authorised by the Principal & Chief Executive)
- Disciplinary action (which may lead to suspension, termination or withdrawal)
- If the action is suspected to be illegal then the incident will be referred to the relevant authorities.

6.2 If a user suspects misuse of technology they should report this immediately to the e-Safety coordinator (Appendix 1 - Procedure for responding to e-Safety Incidents).

6.3 All users should be aware of their legal obligations, which include:

- Copyright, Designs and Patents Act 1988
- Computer Misuse Act 1990
- Malicious Communications Act 1997
- Protection from Harassment Act 1997
- Data Protection Act 1998
- Counter Terrorism and Security Act 2015

7. Advice and Guidance

7.1 Users may obtain advice and guidance from and member of the IT Services Team or by contacting the IT Servicedesk, Tel 02392 88 2800

8. Links to other Policies

8.1 Health & Safety Policy, Child Protection Policy, Staff & Student Disciplinary Policies.