FUTURE ACADEMIES – STUDENT IT ACCEPTABLE USE POLICY

<table>
<tr><td colspan="4"><b>Document control table</b></td></tr>
<tr><td colspan="2"><b>Document title:</b></td><td colspan="2">Student IT Acceptable Use Policy</td></tr>
<tr><td colspan="2"><b>Author (name & job title):</b></td><td colspan="2">Shanaaz Price
Governance and Compliance Officer</td></tr>
<tr><td colspan="2"><b>Version number:</b></td><td colspan="2">V1</td></tr>
<tr><td colspan="2"><b>Date created:</b></td><td colspan="2">October 2017</td></tr>
<tr><td colspan="2"><b>Date approved:</b></td><td colspan="2">November 2017</td></tr>
<tr><td colspan="2"><b>Approved by:</b></td><td colspan="2">Governing Body</td></tr>
<tr><td colspan="2"><b>Review information:</b></td><td colspan="2">This document is reviewed internally annually, and is reviewed by the Board of Directors every two years.</td></tr>
<tr><td colspan="2"><b>Last internal review:</b></td><td colspan="2">October 2018</td></tr>
<tr><td colspan="2"><b>Last review by Governors/Directors:</b></td><td colspan="2">N/A</td></tr>
<tr><td colspan="4"><b>Document History</b></td></tr>
<tr><td><b>Version</b></td><td><b>Date</b></td><td><b>Author</b></td><td><b>Note of revisions</b></td></tr>
<tr><td>V1</td><td>October 2017</td><td>SP</td><td></td></tr>
</table>

CONTENTS

1. INTRODUCTION

These Guidelines and Regulations apply to all IT facilities and resources across all Future Academies schools including open access and course related and classroom based facilities. The Trust takes very seriously misuse of IT facilities and resources and will take sanctions if any concerns are raised by internal or external parties.

The computer network is provided to support learning and teaching. Students may use a variety of applications and files, make use of storage, scanning and printing facilities as well as interact with other computers and communicate and work with other people by sending and receiving messages. Students are responsible for their own actions in accessing and using the Trust's computer and e-learning resources. The use of the Trust's facilities is a privilege and not a right.

2. SCOPE

The Student IT Acceptable Use Policy applies to all users of Future Academies computer network, and it applies to the use of any of the Trust's computers, wherever they are physically located. The Policy also applies whenever data is transmitted over the network via a privately-owned computer or device, wherever the machine is physically located.

3. ACCESS TO COMPUTER RESOURCES

The Trust IT resources are available for use by any student enrolled at a Trust Academy. Access to the Trust computers is controlled by personal username log-on. You will be provided with a user name, email address and password which you can use to logon to your local Academy network. You must never give your password to anyone and you must never log on to a computer for someone else to use, or use another person's password. Valid users are responsible for all activity on their own user account, even if carried out by another person. Any user found to be using another persons username to gain access, will be subject to disciplinary action. Trust or Academy management retains the right to reset passwords - this will be recorded by the Academy IT department for auditing purposes. Students are not allowed to lock their PC workstations and leave them unattended.

Computer use can be monitored by the local Academy IT Team to determine appropriate use. Internet use is logged and recorded by the IT Team to enable follow up investigation of sites visited, files and emails if there is reason to suspect misuse of the network. Therefore you should not expect that files or emails stored on the network will be private. Internet and email filtering software is installed to restrict access, as far as possible, to inappropriate or offensive content and to reduce the amount of spam or junk mail. This is reviewed and updated regularly, though there can be no guarantee that unsuitable material is never available to users.

If you open a webpage or receive an email that is offensive to you or others, racist, illegal, obscene, misleading or if you are in any way unsure or suspicious about it, report it to a member of staff immediately.

4. ACCEPTABLE USES OF IT RESOURCES

- To support your study or other Academy related work;
- Sending or receiving personal email;
- Recreational use, as long as it does not prevent others from using the computers for an academic related activity.

5. UNACCEPTABLE USES OF IT RESOURCES

Anyone behaving in a manner likely to disrupt purposeful activities whilst teaching and learning using any IT resource may (at the discretion of a member of staff) have their access restricted.

The following are not permitted:

- Visiting internet sites, making, posting, uploading or passing on material or comments that contain or relate to: offensive or racist messages or images, obscene language, harassing or insulting others, pornographic (including child pornography) promotion of illegal act, terrorist extremism, gambling, damage to computers, computer systems or computer networks, changing machine settings including desktop, printer or monitor settings.
- Uploading or downloading any unauthorised software, in particular hacking, encryption or other system tools.
- Attempting to spread computer viruses or any other malicious software.
- Engaging in spamming or other bulk emailing.
- Internet chat or File Transfer Protocol facility, unless this forms part of a lesson supervised by a member of staff.
- Violation of copyright laws. This includes copying material from a website and passing it off as your own work.
- The downloading and/or distribution of music and video files for which licence fees have not been paid also constitutes an infringement of copyright, trademark and intellectual copyright, and is illegal.
- Attempting to load additional software, or attempting to tamper with the default settings for PC's on the Academy network. Software applications available to users are limited to those set out on the PC desktop and the start menu.
- The playing of software-based games, including those on or from the Internet, is not allowed, unless part of a supervised lesson.
- Inappropriate saving, to the network, of personal photos, music, video or other data.
- Inappropriate use of social media whereby information is communicated that brings the reputation of the Trust or Academy into disrepute.

6. PRIVATELY OWNED DEVICES INCLUDING LAPTOPS, NETBOOKS, TABLETS AND PHONES

All rules of usage for internet access and computer usage continue to apply. Students should ensure that their machines are properly protected against viruses.

The Trust cannot accept responsibility for any damage, howsoever caused, to computers or their contents as a result of being connected to the Academy network. It is the responsibility of the owner to ensure that there is a licence for all software installed on privately owned equipment. You will need to have your electrical equipment PAT tested by the Academy if you use our mains electricity supply or network portals. PAT tests are carried out by Facilities staff.

Inappropriate material accessed off-site should not be brought into Trust and shared with others.

Students should exercise care when communicating online or using social networking sites particularly in relation to the Trust and existing or past students or members of staff. Defamatory comments or inappropriate use of materials, including text, photos, images, will be challenged and could lead to disciplinary action. Mobile phones or other recording devices must not be used to record still or moving images or record sound on Trust premises or Academy related activities without the permission of a member of staff. If permission is gained, the recording is for the sole use of the student to support their learning and must not be used on any other platform. Mobile phones should not be used to send offensive messages which harass, insult or attack others.

7. SANCTIONS

The Trust takes the rules set out in the Student IT Acceptable Use Policy very seriously. Any student breaking the rules may be subject to disciplinary action. In extreme cases legal action may be taken.
Incidents which appear to involve deliberate access to websites, newsgroups or online groups that contain the following materials will be reported to the Police:

- Images of child abuse (images of children apparently under 16 years of age) involved in sexual activity or posed to be sexually provocative;
- Adult material that potentially breaches the Obscene Publications Act;
- Criminally racist material in the UK;
- Terrorist extremism;
- Any unauthorised access or use of Trust computing and/or network systems which is in violation of the Data Protection Act or the Computer Misuse Act may be subject to criminal prosecution.

8. MANAGEMENT AND MONITORING

The Trust has software and systems in place to filter and record all Internet usage from Trust devices. These systems are capable of recording (for each and every user) each action performed. The filtering software used by the Trust can prevent access to inappropriate sites. The logging and recording of internet access can identify inappropriate use of the Internet.
The Trust reserves the right, as always, to inspect any and all files stored on computers in all areas of the network in order to assure compliance with policy. The Trust may also review Internet activity and analyse usage patterns where there is cause to suspect inappropriate use. Auditors (internal or external) have the right to access any computer files and systems in the performance of their duties.

Staff may also use software to monitor student usage of the Internet or computers in their teaching areas. If a student finds him/her connected accidentally to a site that contains illegal, sexually explicit or offensive material, or any material that they were not expecting they must disconnect from that site immediately and inform a member of staff.

a. Electronic devices of all kinds that are brought in to Academy are the responsibility of the user. The Academy accepts no responsibility for the loss, theft or damage of such items. Nor will the Academy accept responsibility for any adverse health effects caused by any such devices, either potential or actual.

1. Students' Use of Personal Devices

a. Mobile phones should be switched off and at the bottom of the student's bag at all times. If a student breaches the Academy policy then the phone or device will be confiscated and will be held in a secure place in accordance with the Academy policy.

b. Phones and devices must not be taken into examinations. Students found in possession of a mobile phone during an exam will be reported to the appropriate examining body. This may result in the student's withdrawal from either that examination or all examinations.

c. If a student needs to contact his/her parents/carers they will be allowed to use an Academy phone. Parents are advised not to contact their child via their mobile phone during the Academy day, but to contact the Academy office. Students should protect their phone numbers by only giving them to trusted friends and family members. Students will be instructed on safe and appropriate use of mobile phones and personal devices and will be made aware of boundaries and consequences.

9. REVIEW OF POLICY

The procedures in this Policy will be subject to ongoing review and modification in order to keep up with advances in technology.