Acceptable Use Policy – Students
### Document Management Information

<table>
<thead>
<tr>
<th>Applicable to:</th>
<th>All staff in all Academies and Central Support Services including individuals employed by the Trust, contractors and agency staff. All Members and Trustees.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dissemination:</td>
<td>The policy will be available to staff via the Trust’s Policy Centre and to parents and students via the website.</td>
</tr>
<tr>
<td>Implementation:</td>
<td>Applicable to all DRET academies</td>
</tr>
<tr>
<td>Training:</td>
<td>On request</td>
</tr>
<tr>
<td>Review Frequency:</td>
<td>The policy will be reviewed every three years. The policy will also be reviewed earlier if needed in the light of new evidence/legislation/guidance</td>
</tr>
<tr>
<td>Policy Author:</td>
<td>George Selby, Data Protection Officer</td>
</tr>
<tr>
<td>Executive Policy Owner:</td>
<td>Mark Neild, Deputy Chief Executive</td>
</tr>
<tr>
<td>Approval by:</td>
<td>Level 3 (Executive)</td>
</tr>
<tr>
<td>Approval Date:</td>
<td>22 June 2020</td>
</tr>
<tr>
<td>Next Review Due:</td>
<td>May 2023</td>
</tr>
</tbody>
</table>

### Revision History

<table>
<thead>
<tr>
<th>Document version</th>
<th>Description of Revision</th>
<th>Date Approved</th>
</tr>
</thead>
<tbody>
<tr>
<td>V0.1</td>
<td>Version for Executive Review</td>
<td>May 2020</td>
</tr>
<tr>
<td>V1.0</td>
<td>Approved version</td>
<td>22 June 2020</td>
</tr>
</tbody>
</table>
Contents

Contents

1. Introduction ......................................................................................................................... 4
2. Policy Scope ......................................................................................................................... 4
3. Definitions ............................................................................................................................. 4
4. General Statement on Acceptable Use - Students ............................................................... 4
5. Internet Services ..................................................................................................................... 5
6. Security .................................................................................................................................. 5
7. Using Social Media .................................................................................................................. 5
8. Using a personal Mobile Device for Work Purposes (“BYOD”) ............................................. 5
9. Care of Equipment .................................................................................................................. 6
10. Reporting and Consequences of Non-Compliance .............................................................. 6
11. Related Policies ................................................................................................................... 6
1. Introduction

1.1 This Policy provides the guidelines of acceptable use of Information Communications Technology (ICT) equipment and facilities within The David Ross Education Trust.

1.2 Digital technologies have become integral to the lives of children and young people, both within schools and outside school. These technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. Young people should have an entitlement to safe internet access at all times.

1.3 This Acceptable Use Policy is intended to ensure:

- that young people will be responsible users and stay safe while using the internet and other digital technologies for educational, personal and recreational use.
- that academy systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.

1.4 The Trust will try to ensure that students will have good access to digital technologies to enhance their learning and will, in return, expect the students to agree to be responsible users. Users of the Trust/school’s systems should not have any expectation as to the privacy of their activities whilst using them.


2. Policy Scope

2.1 This policy applies to students within the Trust.

2.2 It is the responsibility of all individuals in the Trust to familiarise themselves with this policy and comply with its provisions.

3. Definitions

3.1 Trust means all Academies within the David Ross Education Trust, as well as Head Office and central services operations.

3.2 Executive Leadership Team means the Chief Executive Officer (“CEO”) and the direct line management reports of the CEO (the “Directors”).

4. General Statement on Acceptable Use - Students

4.1 You agree not to upload, download, post, email or otherwise transmit or store anything that:

- is unlawful, harmful, threatening, abusive, harassing, tortuous, defamatory, vulgar, obscene, libellous, invasive of anyone’s privacy, hateful or racially, ethically or otherwise objectionable.
- you do not have the right to transmit.
- is "junk mail," "spam," "chain letters" or similar
- contains software viruses or any code designed to damage computer systems.

4.2 They also will not use the systems to
• impersonate any other person.
• interfere with or disrupt the IT service.
• collect or store personal information about other people.
• undertake any trading or gambling, other action for personal financial gain, or political purposes unless as part of an agreed curriculum project.
• store or use any unauthorised software.

5. Internet Services

5.1 We expect you to act responsibly in accessing the internet and to report any offending material to staff. Accessing inappropriate material over the internet is a serious disciplinary matter. All users should be aware that internet use is monitored.

6. Security

6.1 You will be given a unique ID and password that will allow you to access your account. They are your responsibility and not to be shared with anyone for any reason.

7. Using Social Media

7.1 When using social media students should ensure that anything associated with them is consistent with their being a student at the school.

8. Using a personal Mobile Device for Work Purposes (“BYOD”)

8.1 The use of any personal devices in your academy is something that can only be allowed with the permission of the school. There is no automatic right for any student to use a smartphone or computer in school.

8.2 When allowed it is conditional on agreement to the following:

• If your computer, smartphone or tablet is connected to the school’s IT systems then it is covered by the same rules for Acceptable Use as the school’s own equipment regardless of who it belongs to.
• The school takes no responsibility for storing, maintenance or security of your device.
• Personal IT devices may not be used in any way that is disruptive or not conducive to a positive working environment.
• No effort may be made to get around the security and filtering arrangements put in place by the Trust. Any personal mobile device must be secured via a Pin Code and have all available security features on the phone enabled before any connection to Trust systems including Wifi. There is an expectation, where possible, for any device to be connected to the Trust systems under the supervision or awareness of the IT Team. Where this is not possible, any device connected to Trust systems must have all the latest security patches installed and a recognised Antivirus system installed before any connection to the Trust system is made, it is the owner’s responsibility to ensure this is the case. Any device that does not meet this criteria will be removed from the Trust systems. Security systems and passwords may change at short notice which may require personal devices to be re-connected.
• The owner is responsible for making sure the device is safe to use.
• Some Academies may only allow particular types of device on the system and their decision is final.

• The school has no responsibility for supporting any particular type of system. Technology changes and a new type of device may not be compatible with our services, or an older one may no longer be supported.

• The school reserves the right to withdraw access to its systems without notice.

9. Care of Equipment

9.1 Equipment must always be looked after with care. The Trust reserves the right to charge the replacement cost of any items damaged by the user.

10. Reporting and Consequences of Non-Compliance

10.1 Non-compliance with this policy may result in disciplinary action being taken.

11. Related Policies

11.1 This policy is related to the following other Trust policies:

• Data Protection Policy