

<b>Policy Title:</b>	<b>ICT Equipment, Email and Internet Use for Students</b>
<b>Policy Reference:</b>	<b>TOA089</b>
<b>Description:</b>	<b>This document provides a framework of protocols for the use of email and the internet by students of the Academy</b>
<b>Status:</b>	<b>Non-Statutory</b>
<b>Category:</b>	<b>Student</b>
<b>Contact:</b>	<b>Name: Matthew Brandish Title: OX4 Director Tel No: 01865 774311</b>
<b>Version:</b>	<b>V1.5</b>
<b>Other relevant TOA polices</b>	<b>TOA007 Attitudes to Learning</b>
<b>Approved by the Governing Board on:</b>	<b>4 September 2020</b>
<b>Date for Review:</b>	<b>August 2022</b>

## Change Record

<b>Vers ion</b>	<b>Date</b>	<b>Description</b>
<b>1.1</b>	<b>September 2012</b>	<b>Policy review</b>
<b>1.2</b>	<b>March 2104</b>	<b>Update</b>
<b>1.3</b>	<b>June 2016</b>	<b>Reviewed &amp; Update of contact name</b>
<b>1.4</b>	<b>August 2018</b>	<b>Reviewed and updated with current working practices</b>
<b>1.5</b>	<b>August 2020</b>	<b>Reviewed and point 13.3 updated</b>

## Index

		Page
1.	Introduction	3
2.	Policy Statement	3
3.	Procedures and Expectations	4
4.	Emailing	5
5.	News Group	5
6.	Use of Social Media sites	5
7.	Mobile Phones	6
8.	Theft, Vandalism and Wilful Damage to ICT Facilities	7
9.	Authorisation and Access	7
10.	Risks	7
11.	How Filtering will be Managed	8
12.	Introduction of the Policy to Students	8
13.	The Academy's ICT Security	8
14.	Complaints	9
15.	Support for Parents and Carers	9
16.	Monitoring, Evaluation and Review	10
Annex 1	Code of Conduct for Student Use of the Academy ICT Equipment, Network, and the Internet	11

# **Student ICT Equipment, Email and Internet Use**

## **1. Introduction**

1.1 The purpose of internet use in the Academy is to raise educational standards, to promote student achievement, to support the professional work of staff and to enhance the Academy's management information and business administration systems.

1.2 The internet is an essential element for education, business and social interaction. The Academy has a duty to provide students with internet access as part of their learning experience.

1.3 Internet use is a part of the statutory curriculum and a necessary tool for staff and students.

1.4 Internet access is an entitlement for students who show a responsible and mature approach to its use.

1.5 This policy also covers the use by students of external software and services accessed via the internet.

## **2. Policy Statement**

2.1 The Academy provides internet access which is designed expressly for student use and includes filtering appropriate to the age of students.

2.2 Internet access is planned to enrich and extend learning activities. Access levels are reviewed to reflect the curriculum requirements and age of students.

2.3 Staff will guide students in on-line activities that will support the learning outcomes planned for the students' age and maturity.

2.4 Students are educated in the effective use of the internet in research, including the skills of knowledge location, retrieval and evaluation.

### **3. Procedures and Expectations**

#### **Monitoring Information**

3.1 If students discover unsuitable sites, the URL (address) and content must be reported to their teacher and/or the IT Support Department who will ensure that the site/s are blocked by the Internet Service Provider.

3.1 The Academy will ensure that the use of internet derived materials by students complies with copyright law.

#### **Access to Academy ICT Systems**

3.2 Access to the Academy computer network, including the internet, is via an individual user account which has a unique user name and password.

3.3 When students are given access to the academy network they are responsible for the security of their account and must not allow the account to be used by any other person.

3.4 Personal passwords should be kept confidential and changed when the system prompts you to do so. When leaving a device unattended, students should ensure that they log off or lock the system to prevent unauthorised users using their account in their absence.

3.5 Students must not download, load or install software, shareware or freeware. The IT department will ensure that all software installed has a current licence.

3.6 Students must not load any data from portable USB devices

3.7 Students must not copy others' work or intrude in others' files.

3.8 Students must be aware of copyright laws when copying or downloading any materials from the internet

#### **Misuse of the Academy ICT Systems**

3.9 Misuse of the Academy ICT system will be considered to be a serious disciplinary offence and will be dealt with within the framework of The Oxford Academy Attitudes to Learning policy.

3.10 Misuse of the Academy ICT system by transmission (or receipt) of any material in any of the following categories will not be tolerated:

- Defamatory
- Offensive

- Untrue or malicious
- In breach of copyright
- Bringing the Academy into disrepute

3.11 A risk assessment will be carried out by their teacher before students are allowed to use a new technology in school.

3.12 Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in the Academy is allowed

## **4. Emailing**

- Students may only use approved email accounts on the Academy system
- Students must immediately tell a member of staff if they receive an offensive email
- Students must not reveal personal details of themselves or others in email communication, such as address or telephone number, or arrange to meet anyone they do not know
- Students should not communicate with strangers at anytime via email or the internet as they may represent a danger to them and to other students
- Whole-class or group email addresses should only be used for teaching and learning purposes
- Access in the Academy to external personal email accounts is not permitted
- Personal social email use is not permitted
- Emails sent to an external organisation should be written carefully and authorised before sending, in the same way as a letter written on Academy headed paper
- The forwarding of chain letters is not permitted.

## **5. News Group**

5.1 News Groups will not be made available to students unless an educational requirement for their use has been agreed by the Headteacher.

## **6. Use of Social Media Sites**

6.1 Students must not access public or unregulated social media web sites or chat rooms either through Academy IT or personal devices where Academy wi-fi is being used

6.2 Students must never use these applications for personal or private purposes during Academy hours. Failure to adhere to this will be regarded as a serious disciplinary offence.

6.3 Students should use only regulated educational chat environments. This use will be supervised and the importance of chat room safety emphasised.

Useful Link - <https://www.gov.uk/government/publications/child-safety-online-a-practical-guide-for-parents-and-carers/child-safety-online-a-practical-guide-for-parents-and-carers-whose-children-are-using-social-media>

6.4 Students must not allow Academy staff to become “friends” on the student’s social networking pages.

6.5 Students should also consider who can access their social networking pages and be careful about the content included thereon.

6.6 Students should also be careful about posting comments about other students, members of staff and/or the Academy as this will be treated as bullying and will lead to disciplinary action.

Useful Link  
[https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment\\_data/file/623895/Preventing\\_and\\_tackling\\_bullying\\_advice.pdf](https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/623895/Preventing_and_tackling_bullying_advice.pdf)

Page 17 - Cyber-bullying and online safety.

## **7. Mobile Phones**

7.1 All students will be told when they are allowed to use their mobile phones during the Academy day (see TOA007 Attitudes to Learning Policy).

7.2 The sending of abusive or inappropriate text messages is forbidden, whether through the internet or mobile technology.

Useful Link  
[https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment\\_data/file/623895/Preventing\\_and\\_tackling\\_bullying\\_advice.pdf](https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/623895/Preventing_and_tackling_bullying_advice.pdf)

Page 17 - Cyber-bullying and online safety.

## **8. Theft, Vandalism and Wilful Damage to ICT Facilities**

8.1 ICT facilities represent a considerable financial investment by the Academy. Theft and vandalism deplete the Academy's resources and are detrimental to the learning of students.

8.2 Students are expected to treat all Academy facilities, including ICT facilities, with respect.

8.3 Students must not use rooms containing ICT facilities unless a member of staff is present and has given permission for the ICT to be used

## **9. Authorisation and Access**

9.1 The Academy will keep an up-to-date record of all students who are granted internet access.

9.2 Students must apply for internet access individually by agreeing to abide by the Code of Conduct for Student use of the Academy ICT Equipment, Network, Learning Platform and the Internet. See Annex 1.

9.3 Parents will be asked to sign and return a consent form at the end of the Code of Conduct. See Annex 1.

## **10. Risks**

10.1 In common with other media such as magazines, books and video, some material available via the internet is unsuitable for students. The Academy will take all reasonable precautions to ensure that users access only appropriate material. However, due to the international scale and linked nature of internet content, it is not possible to guarantee that unsuitable material will never appear on an Academy computer. The Academy cannot accept liability for the material accessed, or any consequences of internet access.

10.2 The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990.

Methods to identify, assess and minimise risks will be reviewed regularly.

Compliance with the policy will be monitored.

## **11. How Filtering will be Managed**

11.1 The Academy will work in partnership with parents; the DfE, the LEA and the Internet Service Provider to ensure systems to protect students are reviewed and improved.

11.2 If staff or students discover unsuitable sites, the URL (address) and content must be reported to the IT Support Department who will ensure that the unsuitable site is blocked by the Internet Service Provider. Students should report the occurrence immediately to their teacher who will report it to the IT Support Department.

11.3 The Academy will manage the configuration of their filtering, utilising both educational and technical experience.

11.4 Teaching and IT Support staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

11.5 Filtering strategies will be selected by the Academy, in discussion with the filtering provider where appropriate. The filtering strategy will be selected to suit the age and curriculum requirements of the student.

## **12. Introduction of the Policy to Students**

12.1 Students will be informed that internet use will be monitored.

12.2 Instruction in responsible and safe use will precede internet access.

## **13. The Academy's ICT Security**

13.1 The Academy ICT systems are reviewed regularly with regard to security.

13.2 Virus protection is installed and updated regularly.

13.3 Security strategies are discussed with our contractor Dataspire and service provider RM and implemented as appropriate.

13.4 Personal data sent over the internet is encrypted or otherwise secured.

13.5 Use of portable media such as memory sticks and other USB memory devices is not allowed.

13.6 Unapproved system utilities and executable files will not be allowed in students' work areas or attached to email.

13.7 Files held on the Academy's network will be regularly checked.

## **14. Complaints**

14.1 Students and parents are able to access the Complaints Procedure through the Academy's website. A hard copy can be obtained from the main school Reception

14.2 Responsibility for handling incidents is delegated to the Deputy Headteacher with Pastoral responsibility

14.3 The expectation is that students and parents will work in partnership with staff to resolve issues.

14.4 There may be occasions when the police must be contacted. Early contact may be made to establish the legal position and discuss strategies.

14.5 Sanctions available include:

- interview/counselling by Head of Year
- informing parents or carers
- removal of internet or computer access for a period, which could ultimately prevent access to files held on the system, including examination coursework.

## **15. Support for Parents and Carers**

15.1 Parents can obtain information on the Academy's ICT protocols on the Academy web site.

15.2 Please email [dpo@theoxfordacademy.org.uk](mailto:dpo@theoxfordacademy.org.uk) if you have a query concerning data protection

15.3 Internet issues will be handled sensitively in order to inform parents without causing undue alarm.

15.4 Useful links

[https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment\\_data/file/623895/Preventing\\_and\\_tackling\\_bullying\\_advice.pdf](https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/623895/Preventing_and_tackling_bullying_advice.pdf)

Page 17 - Cyber-bullying and online safety.

[https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment\\_data/file/623895/Preventing\\_and\\_tackling\\_bullying\\_advice.pdf](https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/623895/Preventing_and_tackling_bullying_advice.pdf)

Please contact the main school Reception if you need a hard copy of these documents or if you would like to make an appointment with your child's Head of Year to discuss an IT issue affecting your child

## **16. Monitoring, Evaluation and Review**

The Governing Board will review this policy at least every two years and assess its implementation and effectiveness. The policy will be promoted and implemented throughout the Academy.

## **Annex 1: Code of Conduct for Student Use of the Academy ICT Equipment, Network, and the Internet**

This simplified Code of Conduct applies to all students, at all times, in and out of Academy hours, whilst using Academy ICT equipment. Please read it carefully.

### **You should:**

- √ only ever use your own system login name, password and email address
- √ only access web sites that are appropriate for, and related to, use in the Academy
- √ be aware that others can see your actions on the internet
- √ be careful of what you say to others and how you say it when communicating online
- √ respect copyright and trademarks. You may not use the words or pictures that you see on an internet site without giving credit to the owner of the site
- √ check with a teacher before opening email attachments or completing online questionnaires or subscription forms
- √ only print files appropriate for, and related to, use in the Academy
- √ save data and electronic documents on the Academy servers appropriate for, and related to, use in the Academy

### **You must not:**

- X give your own system username, password and email address to anyone else or allow them to use your accounts
- X download games or other programmes from the internet or elsewhere
- X use chat rooms or unauthorised web-based social media and email services, eg Facebook, MSN, YouTube, Gmail, etc
- X use or access auction sites, eg eBay
- X try and bypass Academy ICT security measures by using proxy bypass web sites, etc
- X give your name, address, telephone number or any other personal information about yourself or others to anyone you communicate with
- X send, access or display abusive or offensive messages or pictures

- X use or send abusive or offensive language
- X attempt to run or install any software not installed by the Academy IT Support staff
- X waste time on the computer doing things that are not related to your work in the Academy
- X download executables (.exe), zip, (.zip), mp3 (.mp3) files from the internet, email or personal storage devices without direct permission from a member of the Academy IT Support staff
- X connect a digital music player, PDA or other digital storage device including mobile phone to an Academy computer or Academy network without permission from a member of the Academy IT Support or ICT teaching staff
- X store illegally copied music files on any part of the Academy ICT system
- X intentionally cause damage to any part of the Academy ICT system

**You should be AWARE that:**

- you must respect copyright and trademarks. You cannot copy material without giving credit to and obtaining permission from the person and/or company that owns the material. This is, in some cases, illegal
- all use of the computer network(s) is logged and audited including all internet access
- you can be monitored remotely without prior notice or knowledge of the event
- data stored on the Curriculum Network Servers is not private and neither is it 100% secure. All possible precautions are taken to prevent data loss through malicious or accidental actions
- you are responsible for your system usernames (ie if you leave a computer logged on with your username you are responsible for whatever is accessed with your username)
- if appropriate, external agencies, eg **police**, may become involved, as certain activities may constitute a criminal offence
- any accidental accessing of inappropriate material online should be reported immediately to the member of staff in charge
- any deliberate accessing of inappropriate material will lead to disciplinary action in line with the Academy's Attitudes to Learning policy and may involve the police

- any attempt to deliberately view the stored work of other students or staff will lead to disciplinary action in line with the Academy's Attitudes to Learning policy and may involve the police
- a regular check will be made on the Academy ICT network to ensure that no illicit material is taking up valuable resources. All such material will be removed
- failure to abide by this Code of Conduct, as laid out above, will result in loss of access and further disciplinary action may be taken, if appropriate

**Student:**

I agree to abide by the terms of the Code of Conduct for Student Use of Academy ICT Equipment, Network, and the Internet

Signed.....

Date.....

Print Name.....

**Parent:**

As parent or carer, I have read, explained and discussed the Code of Conduct for Student Use of Academy ICT Equipment, Network, and the Internet with my child. I grant permission for my child to access the Academy ICT Equipment, Network, and the Internet. I understand that, if he/she fails to follow this Code of Conduct, access will be withdrawn and I shall be informed.

Parent/Carer's Name.....

Signature.....

Date.....

**Copyright release:**

The Academy may produce web pages, ICT presentations, educational or interest articles for magazines or similar. No student's work or personal photographs will ever be used without their permission but we also need permission from parents/carers. Please rest assured the student's safety will always be of paramount importance; no personal information will be made public. Please sign this copyright release if you are happy for work to be shared in this way.

I give consent for the Academy to publish my child's work subject to strict confidentiality of personal information.

Parent/Carer Signature:.....

Date: .....