Student IT Acceptable Use Policy

1. Introduction

BIRD Conservatoire makes computers, network access, and digital services available to students to support their studies. This policy sets out the rules that apply to use of those facilities. It applies to all students enrolled at BIRD Conservatoire.

Use of BIRD's IT facilities is a privilege, not a right. It can be withdrawn if this policy is breached.

2. Scope

This policy applies to all IT facilities provided or arranged by BIRD, including:

- BIRD-owned computers and equipment on campus
- BIRD's network and internet connection
- Institutional cloud services and applications, including Microsoft 365
- Institutional email accounts and credentials (usernames and passwords)
- Any BIRD system or service accessed from a personal device

The policy applies regardless of where you are when accessing BIRD systems. If you are using a personal device to access your BIRD email, OneDrive, or any other institutional service, this policy applies.

3. Permitted Use

BIRD IT facilities are provided to support your studies. You may also use them for reasonable personal purposes, provided this does not breach any part of this policy, does not interfere with others' use of the facilities, and does not consume excessive network resources.

Personal use is a concession and may be withdrawn at any time.

You must not use BIRD's IT facilities for commercial purposes or personal gain without the prior written approval of the COO or nominee.

4. Your Credentials and Identity

You will be issued with a username and password to access BIRD systems. You are responsible for keeping these secure.

- Do not share your password with anyone, including IT staff and fellow students.
- Do not use an obvious or easily guessed password.
- Do not use the same password for your BIRD account as for personal accounts.
- If you believe your password has been compromised, change it immediately and report this to IT Support.
- Log out properly when you have finished using a BIRD system.
- Do not leave a logged-in session unattended.

You must not attempt to access BIRD systems using someone else's credentials or attempt to obtain or interfere with another person's login details. Attempting to access systems without authorisation is an offence under the Computer Misuse Act 1990.

You must not impersonate another person or disguise your identity when using BIRD IT facilities.

5. Acceptable Behaviour

The same standards of behaviour that apply in the physical world apply online. This includes conduct on social media and in any digital communication that relates to BIRD, its staff, students, or reputation.

You must not use BIRD IT facilities to:

- Access, create, store, transmit or display material that is indecent, offensive, threatening, discriminatory or defamatory
- Harass, bully or discriminate against any person
- Send spam, chain emails, or unsolicited bulk messages
- Impersonate another person or send communications with a false sender identity
- Access, modify or delete information belonging to another person without their permission
- Conduct activities for personal commercial gain

BIRD's policies on equality, diversity and inclusion and its student code of conduct apply equally to your online conduct.

This policy does not restrict the lawful expression of opinions, including views that are controversial or unpopular. Students are free to express personal and academic views on social media, subject to the requirements of the law and the BIRD's student code of conduct. Where there is doubt about whether particular content is consistent with this policy, students are encouraged to seek guidance from BIRD staff before posting.

6. Extremist and Terrorist Material

It is an offence under the Counter-Terrorism and Security Act 2015 and the Terrorism Act 2006 to access, create, transmit, store or display terrorist or extremist material. This prohibition applies to use of BIRD IT facilities. BIRD has a duty under the Prevent strand of the government's counter-terrorism strategy to take steps to prevent radicalisation.

Suspected activity of this nature will be referred to the relevant authorities. For further information, refer to BIRD's Prevent Policy.

7. Copyright

Almost all published material, including music, film, images, software and text, is protected by copyright under the Copyright, Designs and Patents Act 1988. The fact that material is accessible online does not mean it is free to use, copy or distribute.

You must not use BIRD's IT facilities to download, copy, store or distribute copyrighted material without appropriate authorisation. If you are unsure whether your intended use of a piece of material is permitted, seek guidance from the library before proceeding.

8. Data Protection

If you handle personal data belonging to others, for example as part of independent study project, you must comply with BIRD's Data Protection Policy and the requirements of the UK General Data Protection Regulation (UK GDPR) and Data Protection Act 2018.

Email is not a secure channel. You must not use BIRD email to transmit sensitive or personal data unless you have been specifically advised that it is safe to do so.

Do not leave sensitive or personal information visible on your screen when you are away from your computer.

9. Infrastructure and Software

You must not do anything that puts the BIRD's IT infrastructure at risk. This includes:

- Loading software onto BIRD's computers without authorisation from IT Support
- Attempting to reconfigure BIRD equipment or network connections
- Deliberately or recklessly introducing malware or other malicious software
- Attempting to bypass or disable security measures, including antivirus software
- Setting up servers or services on the BIRD network without authorisation

BIRD-managed computers have antivirus software installed and maintained by IT. You must not attempt to disable it. If you suspect a security incident or malware, report it to IT Support immediately.

10. Monitoring

BIRD monitors and logs use of its IT facilities. This is done for the following purposes:

- Detection, investigation and prevention of misuse or breaches of this policy
- Operational management and security of the IT infrastructure
- Compliance with legal obligations

This monitoring activity is itself carried out in accordance with the BIRD's Data Protection Policy and UK GDPR. BIRD will comply with lawful requests for information from law enforcement and government agencies.

You must not attempt to monitor the network or other users' activity without explicit authorisation from the COO or nominee.

11. Personal Devices

If you use a personal device to access BIRD's systems or services, this policy applies to that use. You are responsible for ensuring that your personal device does not put BIRD systems or data at risk, for example by being infected with malware.

You should not store BIRD data on personal cloud services (such as personal Dropbox or Google Drive accounts) unless you have been specifically authorised to do so.

12. Social Media

When posting content about the BIRD, its staff, students, or activities on social media, you are expected to behave in a way consistent with the BIRD's student code of conduct. The prohibitions in section 5 of this policy, including on offensive, discriminatory and defamatory content, apply to social media use.

You must not post content that purports to represent the BIRD's official position without authorisation.

13. Good Practice Guidance

The following is guidance rather than enforceable obligations. You are encouraged to follow it.

- Check your BIRD email regularly, particularly during term time.
- Delete or archive emails once read to keep your mailbox manageable.
- Do not leave sensitive information visible on your screen when stepping away from a computer.
- Be cautious with email attachments and links, particularly from senders you do not recognise.

14. Breaches and Reporting

Breaches of this policy may result in disciplinary. The severity of any action will be proportionate to the nature of the breach. Serious breaches, including unlawful activity, may result in withdrawal of IT access, suspension or expulsion, and referral to law enforcement.

If you become aware of a suspected breach of this policy by another person, you should report it to IT Support. Reports can also be made confidentially through BIRD's student complaints process.

If you accidentally encounter material you believe to be illegal, for example, child sexual abuse material, stop immediately, do not view it again, and report it to IT Support.

15. Document Control

Document type:	Policy		
Document number:	013	Version:	2.0
Department:	IT		
Approved by:	Executive Team	Date approved:	07/07/2026
Effective from:	01/08/2026	Review date:	06/07/2029
Publication:	BIRD website		
Related documents:	Data Protection Policy Student Code of Conduct Student Disciplinary Procedure Prevent Policy EDI Policy		
Documents replaced:	Code of Practice for Use of College PCs and E-Mail		
Notes:	Document retitled as Student IT Acceptable Use Policy. Scope clause added. Monitoring disclosure added. Data protection clause added. Copyright clause added. Disciplinary framing revised. Password guidance expanded. Newsgroups/browsing clause removed. Antivirus guidance updated. Prevent Duty cross-reference strengthened. Social media and personal device use addressed. Infringement reporting route added.		