CONTENT REVIEW ACCEPTED | 5 November 2026

IT Acceptable Use Policy

Version	5.1
Effective date	On approval
Date for review	November 2027
Policy owner	Chief Executive
Reference points	UK GDPR and Data Protection Act 2018 UK Government guidance: Meet the requirements of data privacy regulations Higher Education Statistics Agency (HESA) Data protection notices Information Commissioner's Office (ICO) Data protection guidance Office for Students (OfS) Regulatory expectations on data protection, safeguarding, and student security BIMM University Relevant IT governance and data protection frameworks as NHAM's validating partner
Audience/handling notes	Institutional, Staff, Students, Internal
Dissemination and implementation plan	This policy will be: Published in the Staff Handbook and Student Handbook Covered during staff induction and training Introduced to students during induction Stored in Google Drive for easy reference by all staff and students The Academy Manager is responsible for operational implementation, with oversight from the Governance Committee and the Chief Executive, as part of NHAM's institution-wide commitment to data security, IT governance, and student safeguarding in line with UK legal requirements and BIMM University's standards.
Linked Policies, Procedures and Forms	Staff Handbook, Student Handbook, Student Code of Conduct, Staff Code of Conduct, Student Disciplinary Policy, Staff Disciplinary Policy, Data Protection Policy, Privacy Statement
Date approved	Pending approval

1 Introduction

This Information Security and Acceptable Use Policy sets out the responsibilities of all members of the Notting Hill Academy of Music (NHAM) community in relation to the safe, lawful, and ethical use of Academy-provided IT systems, services, equipment, and networks.

The policy exists to:

- Protect information including personal data, intellectual property, and confidential business information from unauthorised access, alteration, or deletion.
- Ensure lawful and responsible use of NHAM IT systems and equipment, in compliance with the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018, the Computer Misuse Act 1990, the Copyright, Designs and Patents Act 1988, the Equality Act 2010, and the Academy's duties under the Counter-Terrorism and Security Act 2015 (Prevent Duty).
- Support academic and operational activities by ensuring that NHAM's digital environment is safe, secure, and inclusive.
- Align with BIMM University policies, recognising that all NHAM students are registered BIMM University students and therefore subject to relevant BIMM University regulations.

This policy applies to all NHAM staff, students, contractors, visitors, and any third parties granted access to NHAM IT systems or data, whether using Academy-owned devices or personally owned devices connected to Academy systems ("Bring Your Own Device" / BYOD).

All users must also familiarise themselves with NHAM's Data Protection Policy, Privacy Statement, and Guidance on the Use of Generative AI. Breaches of this policy will be dealt with under NHAM's disciplinary procedures and, where applicable, BIMM University's disciplinary regulations.

2 Responsibilities for information security

Information security is a shared responsibility across the NHAM community. Every individual who uses NHAM IT systems, networks, equipment, or data is expected to act lawfully, ethically, and in accordance with this policy.

2.1 All Users

All staff, students, contractors, and authorised third parties must:

- Use NHAM IT systems and equipment only for lawful, authorised, and ethical purposes.
- Protect personal data and confidential information in accordance with the UK GDPR and Data Protection Act 2018.
- Take reasonable steps to prevent unauthorised access to systems or information, including using strong passwords and securing devices.
- Report suspected information security incidents or breaches without delay (see Section 3).
- Comply with the BIMM University IT Acceptable Use Policy where applicable, as all NHAM students are registered with BIMM University.

2.2 Leadership and Governance

- **Chief Executive**: Holds overall accountability for information security at NHAM, including ensuring compliance with legislation and sector best practice. Oversees the implementation of this policy and chairs relevant governance discussions. Ensures annual review and update of this policy.
- **Governance Committee**: Provides oversight of information security risk management, reviews policy effectiveness, and ensures alignment with NHAM's strategic objectives and BIMM University requirements.

2.3 Operational Roles

- **Academy Manager**: Responsible for the operational implementation of information security measures, responding to incidents, and ensuring all users are aware of and trained in policy requirements.
- **Programme Leaders and Line Managers**: Ensure that teams and students under their supervision understand and comply with this policy and have access to appropriate support and training.
- **System Owners**: Responsible for ensuring that security measures are embedded "by design and by default" in any IT systems they manage or procure.

3 Reporting a security concern

3.1 General Principles
All staff, students, and authorised third parties have a duty to promptly report any actual, suspected, or potential information security incident, including but not limited to:

- Loss, theft, or unauthorised disclosure of personal data.
- Unauthorised access to NHAM or BIMM University systems.
- Malware infections, phishing attempts, or suspicious emails.
- Physical security breaches involving IT equipment or confidential records.

Early reporting is essential to reduce potential harm, meet ICO reporting deadlines (within 72 hours for personal data breaches), and protect NHAM's legal and reputational standing.

3.2 How to Report

- Students should report concerns immediately to:
    - The Academy Manager
    - Their Programme Leader, lecturer, or personal tutor

- Staff should report directly to:
    - The Academy Manager
    - Or, in serious cases, the Chief Executive

Reports can be made in person, by email, or via a secure reporting form (available on the NHAM student and staff portals).

If the incident involves a system or service managed by BIMM University, NHAM will liaise directly with BIMM's IT and Data Protection teams to ensure coordinated action.

3.3 Data Breach Definition
Under the UK GDPR and Data Protection Act 2018, a *personal data breach* is any security incident that results in:

- Unauthorised access to personal data.
- Unauthorised alteration or deletion of personal data.
- Loss, theft, or destruction of personal data, whether accidental or unlawful.

This applies to both electronic and paper-based records.

3.4 Immediate Actions
When a security concern arises, the person reporting it should:

1. Stop using the affected device or system (to prevent further damage or loss).
2. Retain any evidence (emails, screenshots, logs) for investigation.
3. Not attempt to investigate independently unless authorised to do so.
4. Report immediately: do not wait to gather all the details before making the initial report.

3.5 NHAM's Response
Once a report is received:

- The Academy Manager will log the incident in the Information Security Register.
- If the incident is a *personal data breach*, the Data Protection Officer (DPO) will assess whether it needs to be reported to the ICO within 72 hours.
- If relevant, affected individuals will be notified in accordance with legal requirements.

- The Academy Manager will contact BIMM's IT or data protection team where BIMM systems or data are affected and agree who leads the response and communications.

4 Infringement

4.1 Overview
NHAM takes breaches of this policy seriously. All staff, students, and authorised third parties are expected to comply fully with its provisions.
Breaches of this policy may also constitute breaches of:

- The Student Code of Conduct or Staff Code of Conduct.
- UK legislation such as the Data Protection Act 2018, Computer Misuse Act 1990, and UK GDPR.
- BIMM University regulations (where applicable).

4.2 Investigation Process

- All alleged breaches will be investigated promptly and fairly.
- Investigations may include technical analysis of systems, review of access logs, interviews, and examination of relevant evidence.
- NHAM may choose not to investigate anonymous reports unless sufficient evidence is provided to warrant action.
- Where systems or data belong to BIMM University, investigations may be conducted jointly with BIMM's IT Security and Data Protection teams.

4.3 Referral to External Authorities

If NHAM reasonably believes that a breach involves unlawful activity, it will:

- Refer the matter to the police or other relevant enforcement agencies.
- Where applicable, inform regulators such as the Information Commissioner's Office (ICO) or Office for Students (OfS).
- Where a breach involves a third-party service provider, notify that organisation in line with contractual and legal obligations.
-

External authority involvement does not prevent NHAM from taking its own disciplinary or contractual action.

4.4 Consequences of Non-Compliance
Breaches of this policy may result in:

- For students: Action under the Student Disciplinary Policy, which could include suspension, loss of IT access, or permanent exclusion.
- For staff: Action under the Staff Disciplinary Policy, which could include dismissal.
- For third-party contractors or visitors: Termination of access to NHAM systems, removal from premises, and potential legal action.

4.5 Mitigating Factors
NHAM will consider:

- The intent behind the breach (deliberate or accidental).
- The seriousness and potential harm caused.
- The individual's cooperation during the investigation.
- Whether the breach was self-reported.

Self-reporting and proactive cooperation may be considered a mitigating factor when determining outcomes.

5 Acceptable and Unacceptable Use Guidelines

5.1 Purpose
These guidelines ensure that all users of NHAM's IT systems, networks, and devices:

- Protect data and privacy in line with UK GDPR and the Data Protection Act 2018.
- Maintain cyber security best practice.
- Act in a way that supports a respectful, safe, and productive academic community.

5.2 Dos – You must:

- Use strong passwords: Create a secure password using three random words with mixed case, numbers, and punctuation (e.g., River-Horse!Moon).
- Change your password immediately if you suspect it is compromised, and at least annually.
- Store data securely: Back up important files to NHAM's approved systems (Google Drive) rather than personal storage devices.
- Report security concerns promptly to your Programme Leader, Academy Manager, or IT support.
- Be alert to phishing and other online scams; verify suspicious messages before acting.
- Be considerate of others when using shared IT resources.
- Follow all related policies (including the Data Protection Policy and Student/Staff Code of Conduct).

5.3 Don'ts – You must not:

- Share your password with anyone or store it in an insecure location.
- Leave NHAM devices unattended while logged in.
- Download or share material from untrusted or illegal sources.
- Waste IT resources (e.g., excessive printing, bulk unsolicited emails).
- Attempt to disable, bypass, or interfere with NHAM's security systems.
- Remove or alter Academy IT equipment without authorisation.
- Access, modify, or delete other people's data without permission.
- Assume that cyber security is solely an "IT responsibility" — it is everyone's responsibility.

5.4 Enforcement
Failure to follow these guidelines may be treated as a breach of this policy and could result in:

- Disciplinary action under the Student or Staff Disciplinary Policies.
- Withdrawal of IT access.
- Referral to law enforcement if illegal activity is suspected.

6 Personal activity, equipment and services

6.1 Personal Activity on NHAM Systems

NHAM provides IT systems, devices, and network access to support teaching, learning, research, and administrative functions.

Personal use is permitted only where it:

- Is reasonable and limited in scope.
- Does not interfere with academic or operational activities.
- Complies with this and all other NHAM policies, as well as applicable UK law.

6.2 Prohibited Personal Use

You must not use NHAM IT systems or equipment to:

- Conduct commercial or for-profit activities unrelated to your role or studies.
- Compete with NHAM's business interests.
- Access, create, download, or share content prohibited under Section 7 (Prohibited Activities).
- Introduce information security risks (e.g., installing unauthorised software, visiting unsafe websites).

NHAM accepts no liability for any loss, damage, or claims arising from personal use of its services or devices, except where caused by the Academy's own negligence.

6.3 Use of Personal Devices for NHAM Activities (BYOD)

If you choose to use your own device (e.g., laptop, tablet, phone) for NHAM work or study, you must:

- Protect it with a password, PIN, or biometric authentication.
- Keep your operating system and apps up to date with automatic updates enabled.
- Install and maintain anti-virus or other security software (both Windows 10/11 and MacOS have built-in tools).
- Connect only via approved NHAM network access methods.

You must not:

- Plug your personal device directly into NHAM's internal network without prior written authorisation from IT Services.
- Store sensitive or confidential NHAM data on a personal device unless it is encrypted and approved for that purpose.
- Disable security software or settings required by NHAM.

6.4 Security Monitoring and Compliance

NHAM reserves the right to:

- Any inspection must be specifically authorised, necessary and proportionate, with the scope and applicable privacy information explained.
- Deny or withdraw network access if a device is found to be insecure.
- Require installation of NHAM's Mobile Device Management (MDM) software to secure access.

If you do not wish to agree to these requirements, you should use only NHAM-provided devices for Academy work.

7 Prohibited activities

All staff and students must use NHAM IT systems, networks, and devices responsibly, lawfully, and in a way that supports the Academy's mission. The following activities are strictly prohibited:

7.1 Illegal or Unlawful Use

You must not:

- Engage in any activity that breaches UK law, including but not limited to the Computer Misuse Act 1990, Data Protection Act 2018, UK GDPR, Copyright, Designs and Patents Act 1988, and the Counter-Terrorism and Security Act 2015.
- Access, create, download, store, or transmit material that is indecent, offensive, threatening, defamatory, or promotes extremism or terrorism.
- Commit or attempt to commit fraud, identity theft, or any other criminal offence.

7.2 Discrimination and Harassment

You must not:

- Access, create, download, store, or transmit material that discriminates against, harasses, or demeans others based on protected characteristics under the Equality Act 2010 (including race, religion or belief, sex, gender reassignment, disability, sexual orientation, age, pregnancy/maternity, or marital/civil partnership status).
- Use NHAM systems for bullying, harassment, intimidation, or any behaviour likely to cause distress or anxiety.

7.3 Security Violations

You must not:

- Deliberately or recklessly compromise the security of NHAM's systems, networks, or devices, including introducing malware, bypassing security controls, or disabling protective software.
- Access, modify, or delete data without explicit permission from the data owner.
- Attempt to monitor, intercept, or scan network traffic without written authorisation from NHAM IT Services.

7.4 Misuse of Resources

You must not:

- Use NHAM services or networks for personal financial gain or to compete with NHAM's business.
- Engage in excessive use of bandwidth or system resources, including mass emailing, cryptocurrency mining, or large-scale unauthorised downloads.
- Install or run unapproved software, servers, or applications on NHAM systems.

7.5 Third-Party Services and Licences

You must not:

- Breach the terms of service or licence agreements for third-party software or platforms provided by NHAM (e.g., Microsoft 365, Google Workspace).

- Share NHAM-licensed software, accounts, or content with unauthorised individuals.

7.6 Academic Integrity and Prevent Duty
You must not:

- Use IT systems in a way that undermines NHAM's academic integrity policies, including plagiarism, unauthorised AI use, or other forms of academic misconduct.
- Access or distribute extremist content except where necessary for approved academic research, and only with prior written approval from NHAM's Governance Committee.

Enforcement
Breaches of this section may lead to:

- Suspension of IT access.
- Disciplinary action under the Student Code of Conduct or Staff Disciplinary Policy.
- Referral to external authorities, including the police, where appropriate.

8 Passwords

Your NHAM password is the key to your account, personal data, and the Academy's systems. It is your responsibility to keep it secure at all times.

8.1 Choosing a Strong Password
When setting or changing your NHAM password:

- Use three random words that are easy for you to remember but hard for others to guess (e.g., Tree-Window-Drum).
- Include a mix of upper and lower case letters, numbers, or punctuation.
- Avoid anything linked to you or NHAM (e.g., names, birthdays, course names).
- Never reuse a password from another account.

Your password must:

- Be at least 10 characters long.
- Be unique to NHAM systems.
- Not be based on a single dictionary word or predictable sequence.

8.2 Keeping Your Password Secure
You must:

- Keep your password confidential, do not share it with anyone, including NHAM staff.
- Change your password immediately if you think it's been compromised.
- Store passwords securely in an encrypted password manager (never on paper or in plain text).
- Use multi-factor authentication (MFA) where available for additional security.

8.3 Password Change Policy

- You are required to change your NHAM password at least once every 12 months.
- You must change it immediately if:
    - You suspect compromise.
    - You receive a temporary password from NHAM IT Services.

8.4 Accountability

You are personally responsible for all activity carried out under your NHAM account.
If someone else accesses NHAM systems using your credentials, with or without your permission, you may be held accountable for their actions.

8.5 Devices and Auto-Login

- Never leave a logged-in NHAM device unattended.
- Lock your screen if you step away, even briefly.
- Do not save your NHAM password in browsers or apps unless using secure NHAM-approved password storage.

Breach of password rules may lead to IT account suspension, disciplinary action under the Student Code of Conduct or Staff Disciplinary Policy, and, where necessary, referral to law enforcement.

9 Your data

NHAM is committed to protecting the confidentiality, integrity, and availability of all information created, stored, or processed using Academy systems, in line with the UK GDPR, Data Protection Act 2018, and our obligations as a BIMM University collaborative partner.

9.1 Ownership and Intellectual Property

- You retain ownership, copyright, and intellectual property rights for the original work you create and store using NHAM systems, unless otherwise agreed under specific course, research, or funding arrangements.
- NHAM retains the right to access and use your work only as required for operational, academic, legal, or regulatory purposes.

9.2 Keeping Your Data Safe

You are responsible for regularly backing up your work to an NHAM-approved storage location (e.g., Google Drive) and ensuring it is appropriately protected.
To keep your data safe:

- Use strong, unique passwords for NHAM accounts.
- Avoid storing sensitive personal data unless necessary for your work or studies.
- Always log out of shared or public devices.

9.3 NHAM Access to Your Data

NHAM may access your stored data only:

- With your consent; or
- Where necessary for:
    - Investigating alleged misconduct or breaches of policy.
    - Responding to a security incident or system failure.
    - Complying with legal or regulatory obligations, including the Prevent Duty and requests from law enforcement.
    - Protecting the safety and wellbeing of students, staff, and the wider community.

Access will always be proportionate, authorised, and logged.

9.4 Monitoring

In line with UK law and sector best practice, NHAM may monitor the use of its networks, systems, and equipment to:

- Maintain IT security and prevent cyber threats.

- Detect, investigate, and respond to breaches of policy or law.
- Ensure compliance with licensing, contractual, and regulatory requirements.
- Uphold our safeguarding responsibilities under the Prevent Duty.

Monitoring will be targeted, proportionate, and compliant with data protection principles.

9.5 Leaving NHAM

When you graduate, withdraw, or defer:

- Your NHAM account will be disabled after a short grace period.
- Your data will be retained only for as long as necessary to meet legal, regulatory, or operational requirements.
- It is your responsibility to make copies of any data you wish to keep before your account is closed.

Breach of this section may result in disciplinary action under the Student Code of Conduct or Staff Disciplinary Policy, and where appropriate, referral to relevant external authorities.

10 Web Filtering

NHAM supports the principles of academic freedom and freedom of speech, as set out in UK legislation, Office for Students regulatory guidance, and BIMM University's Freedom of Speech Policy. Students and staff should be able to access online resources necessary for learning, teaching, research, and creative practice, while ensuring compliance with legal and safeguarding duties.

10.1 Purpose of Web Filtering

Web filtering is in place to:

- Protect NHAM systems, networks, and data from cyber threats (e.g., malware, phishing, ransomware).
- Comply with our statutory Prevent Duty to safeguard individuals from being drawn into terrorism or extremist activity.
- Prevent access to illegal or harmful online content.
- Support a safe and respectful online environment for all students and staff.

10.2 Filtering Rules

- Higher Education (HE) students normally have unrestricted access to lawful online content through NHAM networks, except where filtering is required for security or legal compliance.
- Students under the age of 18 will have additional safeguards in place, including category-based content filters, in line with safeguarding best practice.
- NHAM maintains a blocklist of known malicious or harmful sites (updated regularly) to prevent access to unsafe content.

10.3 Requests for Access

If you require access to a blocked site for legitimate academic, research, or creative purposes:

- Speak to your Programme Leader or lecturer.
- They will liaise with the Academy Manager to assess the request.
- Approval will be based on academic relevance, legality, and safeguarding considerations.

10.4 Monitoring and Privacy

- Web access logs may be monitored in line with UK GDPR, Data Protection Act 2018, and NHAM's Data Protection Policy.
- Monitoring is targeted, proportionate, and for specific purposes such as IT security, legal compliance, or safeguarding.

- Academic activity is not routinely monitored for content unless required by law or in response to a specific concern.

10.5 Review and Oversight
The Governance Committee will:

- Review filtering rules and safeguards annually.
- Ensure that filtering does not unduly restrict lawful academic enquiry or breach academic freedom.
- Consider any feedback or concerns raised by students or staff about online access.

Breach of this section may result in disciplinary action under the Student Code of Conduct or Staff Disciplinary Policy, and, if necessary, referral to relevant external authorities.

11 Enforcement, Monitoring and Review

11.1 Enforcement
- Compliance with this policy is mandatory for all students, staff, contractors, and visitors using NHAM systems, networks, or IT services.
- Any breach of this policy will be investigated in line with NHAM's Student Disciplinary Policy, Staff Disciplinary Policy, or other relevant procedures.
- Where unlawful activity is suspected, NHAM may refer the matter to the police, the Information Commissioner's Office (ICO), or other enforcement authorities, without prejudice to internal disciplinary processes.

11.2 Monitoring
- NHAM monitors use of its IT systems in a targeted and proportionate manner to:
    - Maintain network and data security.
    - Detect and investigate policy breaches, misconduct, or unlawful activity.
    - Fulfil legal obligations, including the Prevent Duty and safeguarding responsibilities.
- Monitoring will be carried out in accordance with the UK GDPR, Data Protection Act 2018, and NHAM's Data Protection Policy.
- Data will be accessed only by authorised personnel and retained only for as long as necessary for the stated purpose.

11.3 Review and Continuous Improvement
- The Governance Committee, in partnership with the Chief Executive and BIMM University, will review this policy at least every two years, or sooner if:
    - There are changes to UK law, regulatory guidance, or sector best practice.
    - Significant technological or security developments occur.
    - Issues or gaps are identified through incident reviews, audits, or user feedback.
- The review process will consider:
    - Compliance with the UK Quality Code, Office for Students regulatory guidance, and relevant BIMM University standards.
    - Feedback from students, staff, and external partners.
    - Opportunities to improve clarity, usability, and effectiveness.

11.4 Reporting and Accountability
- The Chief Executive is the policy owner and is accountable for its implementation and enforcement.

- The Academy Manager is responsible for day-to-day oversight, awareness training, and incident coordination.
- The Governance Committee will receive an annual report summarising:
    - Any significant breaches or incidents.
    - Actions taken to address them.
    - Progress on recommendations for improvement.

13 Applying privacy and fair access

Access to systems and personal devices must be lawful, necessary and proportionate. An IT policy does not by itself authorise unrestricted inspection of a personal device. Explain the purpose, scope and authority for any inspection and consider less intrusive evidence. Use the relevant privacy notice, access controls and an unconflicted authorised decision-maker.

Monitoring must be transparent and limited to stated purposes. Restrict access to logs and record why additional monitoring is necessary. Consider data protection impact assessment where processing is likely to create high risk. Lawful academic material must not be blocked solely because it is controversial.

Report suspected data loss, phishing, account compromise or unlawful access immediately to the Academy Manager through an official channel. Preserve evidence and do not investigate other people's accounts. The manager coordinates containment and notifies the relevant data protection lead and BIMM promptly where their data or systems may be affected. The responsible controller assesses regulator and affected-person notifications, including the statutory 72-hour ICO period where applicable.

Keep sensitive student information in approved restricted storage. Use individual accounts and appropriate authentication. Do not forward case files to personal email or leave full student names and health detail in broadly shared minutes. Access to another organisation's platform is subject to the applicable agreement and permissions.

Do not upload personal, confidential, unpublished student or third-party work to an AI or public service without an approved lawful basis and appropriate agreement. Use AI in assessment only as permitted in the brief and Academic Integrity policy, with an accurate declaration.

Provide notice and a secure means to retrieve personal work before account closure where practicable, taking account of record retention and security. Any IT restriction affecting study requires proportionate academic access arrangements and a route to challenge.