LAINE

THEATRE ARTS

Policies

IT Acceptable Use Policy

IT ACCEPTABLE USE POLICY

1. PURPOSE AND SCOPE

This Acceptable Use Policy (AUP) defines the principles and standards for responsible use of the Information Technology (IT) systems, digital services, networks, and data provided by **Laine Theatre Arts** ("Laine"). It aims to ensure the security, integrity, and lawful use of these resources in alignment with:

- Laine's educational mission and values
- The **Office for Students (OfS)** Conditions of Registration
- Legal and regulatory frameworks applicable to UK higher education

This policy applies to all **students, staff, directors, contractors, visitors**, whether on-site or accessing services remotely.

2. REGULATORY AND LEGAL CONTEXT

This policy is designed to support compliance with:

- **OfS Conditions of Registration**, including:
    - **Condition E2** – Effective management and governance
    - **Condition B2** – Student engagement and support
    - **Condition F1** – Accurate and accessible information to students
- **UK General Data Protection Regulation (UK GDPR)** and **Data Protection Act 2018**
- **Computer Misuse Act 1990**
- **Equality Act 2010** – particularly regarding digital accessibility
- **Prevent Duty Guidance: England and Wales (2023)**
- **Intellectual Property (IP) laws**
- **Cyber Essentials (NCSC)** and **Jisc security standards**
- **JANET Acceptable Use Policy** and **Security Policy**

3. ACCEPTABLE USE

Use of College IT systems and Wi-Fi is permitted for:

ACADEMIC AND PROFESSIONAL PURPOSES

- Teaching, learning and rehearsal-related activity
- Accessing the Virtual Learning Environment and academic resources
- Research and coursework
- Communication with staff and students
- Administrative and operational work

REASONABLE PERSONAL USE

Limited personal use is permitted provided it:

- Does not interfere with academic or professional responsibilities
- Does not incur cost to the College
- Does not breach this policy
- Does not compromise network performance or security

4. UNACCEPTABLE USE

The following activities are strictly prohibited on College devices or via College

Wi-Fi:

ILLEGAL ACTIVITY

- Accessing, downloading or distributing illegal content
- Copyright infringement (including unlawful streaming or file sharing)
- Fraud, hacking, or unauthorised access to systems
- Harassment, stalking or malicious communications

INAPPROPRIATE OR HARMFUL CONTENT

- Accessing or distributing pornographic or extremist material
- Viewing material that is discriminatory, hateful or incites violence
- Gambling, except where legally permitted and incidental

MISUSE OF SYSTEMS

- Attempting to bypass security controls or filtering
- Installing unauthorised software
- Introducing malware or unsafe external storage devices
- Using VPNs to circumvent College safeguards
- Excessive streaming or downloads that impact network performance

DATA MISUSE

- Accessing data without legitimate reason
- Sharing confidential student or staff information
- Removing data from College systems without authorisation
- Using College data for personal or commercial gain

REPUTATIONAL DAMAGE

- Posting defamatory or damaging content about the College
- Impersonating the College or other individuals online
- Using College branding without permission

5. ACCESSIBILITY AND INCLUSION

In line with the **Equality Act 2010** and **OfS Condition B2**, all digital platforms, learning technologies, and online content must meet **WCAG 2.1 AA** accessibility standards.

Laine is committed to ensuring that IT services are inclusive and accessible to all students and staff, including those with disabilities or additional needs.

6. DIGITAL WELLBEING AND ONLINE CONDUCT

Users must:

- Engage respectfully in digital spaces, including forums, video calls, and social media.

- Avoid conduct that may harm others' mental health or sense of safety online.
- Use institutional channels (e.g. email, Blackboard and SIS systems) professionally.

7. USE OF PERSONAL DEVICES ON COLLEGE WI-FI

When using personal devices on College Wi-Fi, users must:

- Comply with this policy
- Ensure devices have up-to-date security software
- Not create unauthorised Wi-Fi hotspots
- Not connect unauthorised hardware to the network

The College reserves the right to restrict or block devices that pose a security risk.

8. CLOUD AND THIRD-PARTY SERVICES

When using cloud platforms (e.g. Google Drive, OneDrive, Zoom, Microsoft office), users must:

- Only store personal or confidential data on approved platforms.
- Ensure data sharing complies with the **UK GDPR and our college GDPR policy**.
- Avoid using third-party services that conflict with Laine's data security policies.

9. RESEARCH, CREATIVE WORK, AND INTELLECTUAL PROPERTY

Any use of IT systems for academic research, coursework, or creative performance must:

- Respect intellectual property laws and institutional IP policy.

- Ensure proper storage of research or original work on secure, backed-up platforms.
- Comply with ethics and consent requirements where applicable.

10. NETWORK AND INFRASTRUCTURE USE

- Users accessing services over the **JANET network** must comply with the **JANET Acceptable Use Policy** and **Security Policy**.
- Excessive use of bandwidth or interference with network performance is prohibited.

11. MONITORING AND PRIVACY

- Laine reserves the right to monitor IT activity where legally justified and proportionate (e.g. safeguarding, investigation of misconduct, cybersecurity threats).
- Any monitoring will comply with data protection and UK human rights laws.
- Users should have no expectation of privacy when using institutional systems for unlawful or unauthorised purposes.

12. REPORTING AND SECURITY RESPONSIBILITIES

All users must:

- Report suspected IT security incidents, phishing, malware, or breaches immediately to senior management team.
- Treat all institutional data with appropriate sensitivity and confidentiality.
- Avoid sharing files or links that could introduce harm to the system.

13. SAFEGUARDING AND WELLBEING

The College recognises that online environments can present safeguarding risks. Concerns relating to online abuse, coercion, or exploitation should be reported through the College's safeguarding procedures.

14. ENFORCEMENT AND DISCIPLINARY ACTION

Violation of this policy may lead to:

- Suspension or restriction of IT access
- Disciplinary investigation and action under staff or student disciplinary procedures
- Reporting to law enforcement in cases of criminal activity

15. REVIEW AND GOVERNANCE

This policy will be kept under review by the **Safeguarding and Prevent Committee**, to ensure alignment with changes to legislation, regulation, or risk profile.

KEY DATA

Version:	3
Approved by:	Safeguarding and Prevent Committee on 11th March 2026 and Senior Management Board on 30th April 2026
Review Interval:	1 Year
Last Review Date:	March 2026
Next Review Date:	March 2027