INFORMATION SECURITY POLICY

Norwich University of the Arts is certified to process and administer U.S. Federal Loans (Title IV).

School Code: **042445**

Federal Aid Queries
Email: fedaid@norwichuni.ac.uk
Telephone: +44 1603 753 133

Last reviewed in Jan 2025

Table of Contents

1. Introduction

1.1. Title IV (T4) is a Federal Student Financial Aid for U.S. citizens or eligible non-U.S. citizens. This funding from the U.S. government helps students pay for college tuition and related expenses.

1.2. Norwich University of the Arts (hereafter referred to as the College) is a participating institution in the Federal Direct Loan Programme (Title IV loans). The U.S. Department of Education has regulatory oversight of these loans, but the funds are directly administered by the College for students wishing to study here.

1.3. This policy specifies how the College ensures information security of systems and student data.

2. Responsibility

2.1. As participants of Title IV loans U.S. system, the College and designated officials have access to sensitive personal information about borrowers. We have a duty of care for that personal information, how it is stored, managed, recorded and processed for the purposes of administering loans.

2.2. The rules and regulations for Title IV Federal Student Financial Aid are set by the U.S. Government and data retention requirements as detailed in the Code of Federal Regulations. The College does not have any discretion to alter these Regulations. As with all student information, the College is also bound by UK Data Protection legislation in how we manage and retain information about students. This is similar to that of U.S. law and the Gramm-Leach-Bliley Act.

3. Security

3.1. <u>College's Systems</u>

3.1.1. The College has robust security systems to ensure information security. All systems are password-protected and monitored in real-time by the Information Technology (IT) Office. Microsoft systems are pre-loaded with SOFOS XTR (Extended Detection and Response System) and Mac systems have Jamf Protect. These security programmes protect the college's systems from any security breaches and limit unauthorised application installs.

3.1.2. At the gateway, the university has a firewall protecting all our systems and also has safeguards in place including a cyber security threat monitoring system with JISC. IT maintains an IT risk register that is updated routinely. The College also runs bi-annually risk assessments, in addition to an annual external penetration testing by JISC.

3.1.3. The above processes ensure that the systems used to access U.S. loan systems and store student data are robust and secure. All

users are also required to complete regular Meta Compliance training to keep up to date with the most recent identified risks.

3.2. U.S. Loan Systems

3.2.1. The Student Aid Internet Gateway (SAIG) is the method by which the College signs up, manages and accesses online portals for processing T4 loans. Our SAIG Agreement includes a provision about how we must protect data and systems that the College uses. The Primary Destination Point Administrator (Primary DPA) takes responsibility for ensuring only required staff have access to the U.S. loan systems.

3.2.2. The College currently accesses the below U.S. loan software and systems –

- EdConnect Software
- EdExpress Software
- FSA Partners Website
- FAA Access to CPS Website
- National Student Loan Data System - NSLDS Website
- Common Origination and Disbursement - COD Website
- Student Aid Internet Gateway - SAIG Enrollment Website

3.2.3. All the above loan software and systems require two-factor authentication (TFA) – a password and an additional time-bound numeric key (security code) received via a registered device (token). All U.S. Loans software are installed by our IT Office on systems belonging to designated staff (Primary Destination Point Administrator and Secondary Destination Point Administrators).

3.3. Access controls

3.3.1. The University's U.S. loan borrowers records are held in various forms:

- Paper files
- Emails
- Electronic records
- Restricted shared folders

3.3.2. Sensitive information such as SSN, credit checks, and financial information is only held in electronic records stored in restricted shared folders to ensure information security. These electronic records are only accessible by designated staff within the International Office who have responsibility for processing FedAid loans.

3.3.3. Emails containing sensitive information such as a student's borrowing ability are password-protected/encrypted to ensure personally identifiable data is secure.

3.4. U.S. Loans regulations

3.4.1. The College is subject to legislation under U.S. law in relation to T4 loans. The Federal Student Aid Handbook Volume 2 – *School Eligibility and Operation*, Chapter 7, *Record Keeping, Privacy & Electronic Processes*, has details about good practice in being compliant with record keeping.

3.4.2. The Gramm-Leach Bliley (GLB) Act: Under our Program Participation Agreement (PPA) and GLB (Public Law 106-102), Norwich University of the Arts must protect student financial aid information, with particular attention to information provided to us by the U.S. Department of Education (USDE) or otherwise obtained in support of the administration of the federal student financial aid (FSA) programs.

3.4.3. Family Educational Rights and Privacy Act (FERPA) deals with requirements relating to the privacy and security of Personally Identifiable Information (PII) in student records. The combination of FERPA and GLB is very similar to that of our own data protection legislation Data Protection Act (2018) and General Data Protection Act (GDPR) (2018).

4. Training

4.1. All College staff must undergo online training for:

- Information Security
- Data Protection
- Equality and Diversity

4.2. In addition to this, staff processing FedAid loans or using T4 loans software are required to undergo relevant training too.

5. Data security Incidents

5.1. The USDE encourage colleges to inform their students about any breaches of security in relation to T4 loan records and information. The USDE may consider any breach of the security of T4 student records and information as a demonstration of a potential lack of administrative capability, for which the University can be fined or lose the institutional licence. The College also has a duty to notify FSA about any T4 loans data breaches to: FSASchoolCyberSafety@ed.gov, with a cc to CPSSAIG@ed.gov.

5.2. In the first instance, all T4 data breaches should be reported immediately to the Head of International (Primary DPA for T4 loans). The Head of International will then liaise with necessary parties, including the Compliance Manager and IT Services Manager. The Information Security Incident reporting procedure will be followed which is located within the College's internal Information Security Policy.

5.3. If you have any complaint about how the College has handled your data, you have the right to file a complaint with the U.S. Department of Education. However, it would be desirable to contact the College's FedAid team in the first instance to resolve it.

6. Related General College Policies

6.1. External:

- The College's Data Protection Policy
- The College's Privacy Notice

6.2. Internal:

- IT Acceptable Use Policy
- Information Security Policy (includes Information Security Incident Reporting Procedure)