THE NORTHERN SCHOOL OF ART

INFORMATION TECHNOLOGY POLICIES & PROCEDURES

2025-26

October 2025

northernart.ac.uk

Contents

1.0 DATA PROTECTION

Introduction

1.1 The Northern School of Art is required to retain certain information about its employees, learners and other users in order to facilitate the monitoring of performance, achievements, and health and safety. It is also necessary to process information so that staff can be recruited and paid, courses organised and legal obligations to funding bodies and government complied with. To comply with the law, information must be collected and used fairly, stored and disposed of safely, and not disclosed to any other person unlawfully. To do this, The Northern School of Art must comply with the requirements of the General Data Protection Regulations 2018 (GDPR). In summary these state that personal data shall:

- Be obtained and processed fairly and lawfully and shall not be processed unless certain conditions are met;
- Be obtained for a specified and lawful purpose and shall not be processed in any manner incompatible with that purpose;
- Be adequate, relevant and not excessive for those purposes;
- Be accurate and kept up to date;
- Not to be kept for longer than is necessary for that purpose;
- Be processed in accordance with the data subject's rights;
- Be safe from unauthorised access, accidental loss or destruction;
- Not be transferred to a country outside the European Economic Area, unless that country has equivalent levels of protection for personal data.

1.2 The Northern School of Art and all staff or others who process or use any personal information must ensure that they follow these principles at all times. In order to ensure that this happens, The Northern School of Art has developed this Data Protection Policy.

Status of the Policy

1.3 This policy does not form part of the formal staff contract of employment nor of the student contract explicitly with The Northern School of Art, but it is a condition of both contracts that The School's regulations and policies must be adhered to. A failure to follow the policy may result in disciplinary proceedings.

1.4 Any members of staff or learners who consider that the policy has not been followed in respect of personal data about themselves or about other data subjects should raise the matter with the Data Protection Officer (see 1.22) initially. If the matter is not resolved it should be raised as a formal complaint or grievance.

Definitions

1.5 Definitions are derived from the GDPR and are set out below:

Privacy Statement – a statement by The Northern School of Art which sets out the reasons why personal data is being collected, on what basis it is collected, how long it will be stored, etc.

ICO – Information Commissioners Office

Lawful basis – GDPR defines 6 lawful bases for data collection and processing these are set out here:

i. Consent: the individual has given clear consent for you to process their personal data for a specific purpose.

ii. Contract: the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract.

iii. Legal obligation: the processing is necessary for you to comply with the law (not including contractual obligations).

iv. Vital interests: the processing is necessary to protect someone's life.

v. Public task: the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.

vi. Legitimate interests: the processing is necessary for your legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests. (This cannot apply if you are a public authority processing data to perform your official tasks.)

Special Category Data - is more sensitive than standard contact information, and so needs more protection. It includes information about an individual's:

- race;
- ethnic origin;
- politics;
- religion;
- trade union membership;
- genetics;
- biometrics (where used for ID purposes);
- health;
- sex life;
- or sexual orientation.

In particular, this type of data could create more significant risks to a person's fundamental rights and freedoms. For example, by putting them at risk of unlawful discrimination. It does not include criminal records disclosure.

Data Protection Officer - the DPO must be independent, and report to the highest management level – the DPO will monitor internal compliance, inform and advise on your data protection obligations, provide advice regarding Data Protection Impact Assessments (DPIAs) and act as a contact point for data subjects and the supervisory authority.

Notification of data held and processed

1.6 All staff, learners and other data subjects are entitled to know:

- what information the School holds and processes about them and why;
- how to gain access to it;
- how to keep it up to date;
- what the School is doing to comply with its obligations under the GDPR.

1.7 If and when, as part of their responsibilities, staff collect information about other people (e.g. about students' course work, opinions about ability, references to other academic institutions and details of personal circumstances), they must comply with the guidelines for staff.

Responsibilities of Staff with regard to their own personal data

1.8 All staff are responsible for ensuring that:

- Checking that information they provide to the School in connection with their employment is accurate and up to date.
- Informing the School of changes to information which they have provided, e.g. change of address.
- Checking the information that the School will send to them from time to time, which gives details of information kept and processed about them.
- Informing the School of any errors or changes. The School cannot be held responsible for any errors unless the staff member has informed The School of them.

Responsibilities of Students with regard to their own personal data

1.9 All students are responsible for ensuring:

- information they provide to the School in connection with their study is accurate and up to date.
- They Inform the School of changes to information which they have provided, e.g. change of address.

- Checking the information that the School will send to them from time to time, which gives details of information kept and processed about them.
- Informing the School of any errors or changes. The Northern School of Art cannot be held responsible for any errors unless the student has informed The Northern School of Art of them.
- Students who use the School's computer facilities may, from time to time, process personal data. If they do, they must obtain the prior permission of their course or programme tutor

Data Security

1.10 All staff are responsible for ensuring that:

- Any personal data which they hold is kept securely;
- Personal information is not disclosed either orally or in writing or accidentally or otherwise to a third party.
- Any disclosure to a third party can only be by exception and in relation to a legal or contractual duty (for example safeguarding)

1.11 Staff should note that unauthorised disclosure and / or failure to adhere to the requirements set out in 1.12 to 1.17 inclusive below will usually be a disciplinary matter, and may be considered gross misconduct in some cases.

1.12 Personal information must be:

- Kept in a locked filing cabinet; or
- In a locked drawer; or
- Locked room: or
- If it is computerised, be password protected; or
- When kept or in transit on portable media the files themselves must be password protected.

1.13 Personal data should never be stored at staff members' homes, whether in manual or electronic form, on laptop computers or other personal portable devices or at other remote sites. The School accepts that there may be special operational circumstances when staff do keep personal information at home overnight (for example if working at a different campus the next day) – its storage must follow the protection set out in 12 above. Ideally staff should work through VPN in such circumstances rather than on a stand-alone laptop or desktop.

Student's right to be forgotten

1.14 Students and alumni have the right to request that their data is forgotten and not stored. The School will comply with such requests where they do not conflict with relevant contractual and legal duties such as evidence for funding and fees that have been awarded to the School by the DfE, OfS or SLC.

Rights to Access Information

1.15 Staff, students and other users of the School have the right of access to any personal data that are being kept about them either on computer or in other files. Any person who wishes to exercise this right should complete the School "Access to Information" form and give it to the designated Data Protection Officer, or, in the case of a student, to her/his course tutor or lecturer. Forms are available from the main office.

1.16 The School aims to comply with requests for access to personal information as quickly as possible, but will ensure that it is provided within 20 days unless there is good reason for delay. In such cases, the reason for delay will be explained in writing to the data subject making the request.

Publication of School Information

1.17 Information that is already in the public domain is exempt from the GDPR. It is The Northern School of Art's policy to make as much information public as possible, and in particular the School complies with Model Publication Scheme Guidance, Competition and Markets Authority and Department for Education Guidance relating to the availability, transparency and accuracy of public information.

Subject Consent

1.18 In many cases, the School can only process personal data with the consent of the individual. In some cases, if the data is sensitive, express consent must be obtained (special category data). Agreement to the School processing some specified classes of personal data is a condition of acceptance of a student onto any course, and a condition of employment for staff.

1.19 The Northern School of Art will also ask for information about particular health needs, such as allergies to particular forms or medication, or any conditions such as asthma or diabetes. The School will only use the information in the protection of the health and safety of the individual but will need express consent to process in the event of a medical emergency, for example.

1.20 Therefore, all prospective staff and students will be asked to sign a Consent To Process, regarding particular types of information when an offer of employment or a course place is made. A refusal to sign such a form can result in the offer being withdrawn.

Processing Special Category Data

1.21 Sometimes it is necessary to process information about a person's health, criminal convictions, race and gender and family details. This may be to ensure The Northern School of Art is a safe place for everyone, or to operate other School policies, such as the sick pay policy or equal opportunities policy. Because this information is considered sensitive, and it is recognised that the processing of it may cause particular concern or distress to individuals, staff and students will be asked to give express consent for the School to do this. Offers of employment or course places may be withdrawn if an individual refuses to consent to this, without good reason. More information about this is available from the HR Department or Student Services as appropriate.

The Data Protection Officer and the Designated Data Controllers

1.22 The School as a corporate body is the data controller under the GDPR, and the Governing body is therefore ultimately responsible for implementation. However, the designated Data Protection Officer (DPO) and Data Officers who deal with day-to-day matters are:

DPO: Vice Principal (Resources)

Supported by:

Data Officers: MIS Manager, Vice Principals, Academic Registrar

Retention of Data

1.23 The School will keep some forms of information for longer than others. Because of storage problems, information about students cannot be kept indefinitely, unless there are specific requests to do so. In general information about students will be kept for a maximum of 50 years after they leave The School of Art. This will include:

- Name, address (including e-mail address), date of birth;
- academic achievements, including marks for coursework; and
- copies of any reference written.

1.24 All other information, including any information about health, race or disciplinary matters will be destroyed within 6 years of the course ending and the student leaving the School.

1.25 The School will need to keep information about staff for longer periods of time. In general, all information will be kept for 6 years after a member of staff leaves. Some information however will be kept for much longer. This will include information necessary in respect of pensions, taxation, potential or current disputes or litigation regarding the employment, and information required for job references.

Data Breach

1.26 A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes. It also means that a breach is more than just about losing personal data. In the event of any data breach the person discovering the breach must report this immediately to the DPO, or in the absence of the DPO, one of the Data Officers. Such notification must be given details of:

- The nature of the breach, its scale (how many individuals are affected)
- The type and nature of the data affected by the breach
- An assessment of the consequences of the breach (actual and potential)
- Mitigating action taken

1.27 The DPO must notify the ICO within 72 hours of the breach if there is a risk to the confidentiality, integrity or availability of personal data. The DPO must provide the ICO with a description of the nature of the personal data breach including, where possible:

- the categories and approximate number of individuals concerned; and
- the categories and approximate number of personal data records concerned;
- the name and contact details of the data protection officer or other contact point where more information can be obtained;
- a description of the likely consequences of the personal data breach; and
- a description of the measures taken, or proposed to be taken, to deal with the personal data breach, including, where appropriate, the measures taken to mitigate any possible adverse effects.

Conclusion

1.28 Compliance with the GDPR is the responsibility of all staff and students of The Northern School of Art. Any deliberate breach of the Data Protection Policy may lead to disciplinary action being taken, or access to School facilities being withdrawn, or even a criminal prosecution. Any questions or concerns about the interpretation or operation of this policy should be taken up with the designated DPO.

2.0 INFORMATION SECURITY POLICY

Purpose

2.1 This policy outlines The Northern School of Art's approach to information security and provides the guiding principles and responsibilities to ensure The Northern School of Art's security objectives are met.

Scope

2.2 This policy is applicable across The Northern School of Art and individually applies to:

- all individuals who have access to The Northern School of Art information and technologies;
- all facilities, technologies and services that are used to process The Northern School of Art information;
- information processed, in any format, by The Northern School of Art pursuant to its operational activities;
- internal and external processes used to process The Northern School of Art information; and
- external parties that provide information processing services to The Northern School of Art.

Objectives

2.3 The Northern School of Art's objectives for information security are that:

- a GDPR compliance culture is generated and adhered to;
- a culture is embedded to ensure all teaching, research and administration activities consider information security;
- individuals are aware and kept informed of their information security responsibilities;
- information risks are identified, managed and mitigated to an acceptable level;
- authorised users can securely access information to perform their roles;
- facilities, technologies and services adequately balance usability and security;
- implemented security controls are pragmatic, effective and measurable;
- contractual, regulatory and legal obligations relating to information security are met; and
- incidents are effectively managed and resolved, and learnt from to improve our control environment.

Requirements:

2.4 All stored information will need to meet the following requirements

- will be reviewed annually by business area manager to ensure it is still required and only accessible by relevant and appropriate staff.
- is obtained and processed fairly and lawfully and shall not be processed unless certain conditions are met;
- is obtained for a specified and lawful purpose and shall not be processed in any manner incompatible with that purpose;
- is adequate, relevant and not excessive for those purposes;
- is accurate and kept up to date;
- is not to be kept for longer than is necessary for that purpose in line with the retention guidelines from the Data Protection Policy;
- is processed in accordance with the data subject's rights;
- is safe from unauthorised access, accidental loss or destruction;
- is not to be transferred to a country outside the European Economic Area, unless that country has equivalent levels of protection for personal data.

Information Security Policy Framework (ISPF)

2.5 Information is critical to The Northern School of Art's operations and failure to protect information increases the risk of financial and reputational losses. The Northern School of Art is committed to protecting information, in all its forms, from loss of confidentiality, integrity and availability ensuring that:

- information security risk is adequately managed and review of IT systems and business processes are performed where appropriate;
- all relevant information security requirements of The Northern School of Art are covered in agreements with any third-party partners or suppliers, and compliance against these is monitored;
- appropriate information security controls are implemented to protect all IT facilities, technologies and services used to access, process and store The Northern School of Art information;
- all information security incidents are reported in a timely manner via appropriate management channels, information systems are isolated, and incidents properly investigated and managed;
- information security controls are monitored to ensure they are adequate and effective.

Minimum Security Baseline

2.6 The Northern School of Art requires devices connecting to the network to meet the minimum-security baseline in order to protect devices. Devices connecting to the network must comply with the baseline before access to organisation's information resources is granted. The baseline safeguards protect the confidentiality, integrity, and availability of each individual device and other devices connected to the network by reducing the security susceptibility of every device. All staff and students of The Northern School of Art, guests, third parties and any other entities connecting any device to the network are subject to this policy. All network connected devices must be configured to meet the baseline. The baseline security safeguards listed below are the minimum required to protect devices:

- Antivirus software must be enabled, running, and up-to-date on every device.
- Applications and operating system software running on devices must be a supported version.
- The installation of relevant software updates, patches, or upgrades fixing critical or high security vulnerabilities of devices must be prompt.
- As per the IT Systems Use Policy only The Northern School of Art controlled devices are permitted access to the Wired Network.

2.7 To provide the foundation of a pragmatic information security framework, The Northern School of Art will implement a set of minimum information security controls, known as the baseline, either as published by the School's IT Department. Where research, regulatory or national requirements exceed this baseline, controls will be increased at necessary service or project level. Where it is not possible or practicable to meet the baseline, exceptions will be documented to justify the deviation and appropriate compensating controls will be put in place. The baseline will support The Northern School of Art in achieving its information security objectives.

2.8 The School will conduct regular penetration tests and other methods of testing vulnerabilities to ensure the integrity of its systems

2.9 As per the ESFA funding contract for 2024-25, the School is required to have achieved Cyber Essentials certification during the 2024/25 Funding Year and be able to present evidence to the DfE on request.

2.10 The policy and the baseline shall be communicated to users and relevant external parties and linked to from the website.

Responsibilities

2.11 The following bodies and individuals have specific information security responsibilities:

- The Vice Principal - Resources has executive responsibility for information security within The Northern School of Art. Specifically, the Vice Principal - Resources has responsibility for overseeing the management of the security risks to The Northern School of Art's staff and students, its infrastructure and its information. The Vice Principal - Resources is also the Data Protection Officer for The Northern School

of Art and is supported by the MIS Manager, Vice Principals and the Academic Registrar.

- The IT Manager is accountable for the effective implementation of this information security policy, and supporting information security rules and standards, within The Northern School of Art.
- The IT Manager is responsible for establishing and maintaining The Northern School of Art's information security management framework to ensure the availability, integrity and confidentiality of The Northern School of Art's information. The IT Manager will lead on the definition and implementation of The Northern School of Art's information security arrangements.
- Users are responsible for making informed decisions to protect the information that they process.

Compliance

2.12 The Northern School of Art shall conduct information security compliance and assurance activities, facilitated by the School's IT Department, to ensure information security objectives and the requirements of the ISPF are met. Wilful failure to comply with the policy and baseline will be treated extremely seriously by The Northern School of Art and may result in enforcement action on a group and/or an individual.

Data Breach

2.13 A data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes. It also means that a breach is more than just about losing data. In the event of any data breach the person discovering the breach must report this immediately to the Data Protection Officer. Further details on how to report the breach and the actions the Data Protection Officer must take are available in the Data Protection Policy.

Review and Development

2.14 This policy, and supporting ISPF documentation, shall be reviewed by Principalship and updated by the IT Manager on a 2-year basis to ensure that they:

- remain operationally fit for purpose;
- reflect changes in technologies;
- are aligned to industry best practice; and
- support continued regulatory, contractual and legal compliance.

Related Documents

2.15 The following documents are relevant:

- Data Protection Policy
- Staff Data Protection Procedure

3.0 IT ACCEPTABLE USE POLICY

Purpose

3.1 The Northern School of Art (the School) IT Acceptable Use Policy is a School document that a user must agree to follow in order to be granted access to the School network and information technology assets.

3.2 Compliance is indicated by acceptance at enrolment (students) or at appointment (staff)

Scope

3.3 The IT Acceptable Use Policy applies to users who are given full or temporary access to School information technology assets. This includes staff (anyone working full or part-time, whether directly employed or employed by an agency), students, governors, visitors (e.g. inspectors, auditors), etc.

3.4 This Policy covers the use of School IT assets such as computers, peripherals, networking, miscellaneous hardware (this includes photocopiers, telephony and School mobile phones) removable devices, software and data. It also covers IT facilities owned by other organisations or privately owned which the School utilises.

3.5 Users should also be aware that it is a criminal offence in English law to obtain access to any computer system without authorisation or to store and transmit certain types of offensive material (such as pornography) on computer systems. All members of the School are subject to the Regulations of the School and to English law. UK criminal law will be enforced by notifying the authorities whenever it has been broken.

Enforcing

3.6 All users must be made aware of the IT Acceptable Use Policy. Students will be made aware of the Policy during enrolment and staff at appointment. Staff and students must each agree on acceptance to allow access to the institution's IT facilities. A hard copy of the Policy is available on request from the IT department and will also be published on the School VLE (Moodle). Updates to the IT Acceptable Use Policy are ongoing and will be published by email and available on the School VLE (Moodle), initial acceptance indicates acceptance to further updates published to users.

3.7 Students will then be enrolled on the School's student administration system which will automatically generate an account. An account will not be generated without this process being completed.

3.8 Some users may be requested to complete further paperwork in order to complete this process, for example, shared drive requests, etc.

3.9 Any user contravening the IT Acceptable Use Policy may have their rights to the School's systems revoked and/or face disciplinary actions; this is at the discretion of the Principalship Team.

Responsible Use:

3.10 Strict Rules: Users are not under any circumstances permitted to use the School's IT Assets for any of the following:

a. Any unlawful activity

b. The creation, transmission, storage, downloading or display of any offensive, obscene, indecent, or menacing images, data or other material, or any data capable of being resolved into such images or material.

c. The creation or transmission of material which is designed or likely to cause annoyance, inconvenience or needless anxiety, or to harass another person or persons.

d. The creation or transmission of defamatory material about any individual, group or organisation.

e. The sending of any email or any other method of electronic correspondence that does not correctly identify the sender of that email or attempts to disguise the identity of the computer/individual from which/whom it was sent.

f. The sending of any message appearing to originate from another person, or otherwise attempting to impersonate another person.

g. The possession of an account designed to mislead others to the identity of the account holder, to impersonate an individual or to use an account to anonymously communicate with another, specifically to cause annoyance, inconvenience or needless anxiety, or to harass a person or persons.

h. The creation, access or transmission of material in such a way as to infringe copyright, trademark or other intellectual property rights.

i. Private profit, except to the extent authorised under the user's conditions of employment or other agreement with the School; or commercial purposes without specific authorisation from senior management and/or the IT Manager.

j. Gaining or attempting to gain unauthorised access to any facility or service within or outside the School, or making any attempt to disrupt or impair such a service.

k. The corruption or disruption of other users' data

l. The violation of the privacy of other users

m. The disruption of the work of other users

n. To attach personal computers, laptops or any networkable device to the School physical network using a wired network connection without the permission of the IT Manager is expressly forbidden. We encourage the use of wireless

technologies to link using our wireless systems; we would prefer any connection of third-party devices to be wireless rather than wired.

3.11 General Rules, Guidelines and Examples:

a. Users access the network by using a username and password. This password must not be communicated or given to anyone else. Users should also ensure that they log-off after using a computer, or if a computer is left unattended one should either log-off or lock the computer.

b. A User must never use another user's account.

c. Users should not use IT assets for activities not directly connected with employment, study or research in the School. However, it is acceptable for users to have reasonable and limited use for social and recreational purposes. This is when use is not in breach of any other rule(s) in the IT Acceptable Use Policy.

d. The School e-mail should only be used for School-related use, we understand that on some occasions it might be convenient to use the School email for personal use and we accept this ad-hoc use, however we would recommend that users have their own personal email address for their own use, especially when setting up accounts with third parties.

e. Staff members should not use their own personal social networking accounts to communicate with students. They should not "friend" students on their personal Facebook accounts or do similar actions on other social networking sites.

f. Staff users should not print out work on behalf of a student.

g. Staff users should not allow students to use their photocopying/ID card for any purpose.

h. Use of proxies or any other mechanism to bypass the School's web filtering is strictly forbidden.

i. Students and staff must not use or peer-to-peer (P2P) sharing sites (including those used to distribute BitTorrent files) to share or download copyrighted and/or offensive material such as music, software, movies, etc. Students and staff must not install P2P software on any of the School's computers, tablets, telephones, etc. Students and staff are requested to exercise caution when using their own equipment on the School network with P2P software installed, specifically P2P software associated with the sharing of copyrighted and/or offensive material. Any enquiry by a copyright holder or an agency operating on a copyright holder's behalf will be forwarded, where possible, to the individual sharing the copyrighted material.

j. Students will be charged for prints from the IT system; refunds will only be issued for erroneous prints when it is considered that the reason for the error is the responsibility of the School.

k. The School reserves the right to view all print records for staff and students.

l. Uncollected printouts will be removed from the print trays of the photocopiers/printers. Staff and students remain at the photocopier/printer while printing is in progress. If this is not possible for some reason, they should collect printouts promptly.

m. All old data and student work may be cleared from the system at the end of the academic year in line with network management and maintenance practices. Students are advised to back up their work on a regular basis & make sure they have a full back up at the end of the academic year.

n. Users must not play games on School equipment. Games can only be played when they are in context with the purpose of study or research and with the agreement of a member of staff who will supervise the gameplay. Games should not be played on personal devices in studio, lecture theatre or class environments.

o. Users must never load their own software onto the computer, and any user requiring a personal software installation must request the consent of the IT Manager once given software may be installed with assistance and supervision of IT staff.

p. Any damage to systems, data or equipment will not be condoned.

q. Any damage caused to systems or equipment will, at the discretion of the School, be charged to the individual. The School will assess and set the charge amount.

r. Students must not eat or drink near the computers without the express permission of the supervising member of staff. Any user eating or drinking near a computer must take great care when doing so any damage to a computer or piece of equipment may be charged to the individual.

s. Users must not do anything to damage the computer resources, both physically and electronically, e.g. by the introduction of viruses, by tampering with the computer setup, or by hacking into any systems. It is the personal responsibility of all users to ensure that they do not introduce viruses or malicious software into the computer systems. Users should take care when receiving electronic information from an unknown source, specifically attachments of an e-mail.

t. The sending of offensive communications, e.g. emails, social media posts, instant messages, texts, etc. will not be tolerated. Any user sending a message which reasonably causes offence will be subject to normal disciplinary procedures (this includes retaliating against offensive messages sent to you – any offensive message you receive should be reported to a member of staff immediately). If it becomes necessary to investigate such incidents, the IT Manager and other staff as appropriate may access and read communications

u. The use of any form of communication mechanism, for example, email, blogs, social networking, forums etc., to distribute defamatory material about the School, a member of staff or a student is forbidden.

v. The sending of mass unsolicited emails by any user is not permitted. Students who need to mass email should seek permission from their Senior Lecturer who in turn should communicate the request to the IT Manager. Staff members should get in touch with the IT Manager directly.

w. When online, users should be careful as to what they disclose to others. Users should remember that email is not private information and anything they send might be read or distributed by another person. Users should also be aware of maintaining privacy settings and limiting personal information on publically accessible websites, it is recommended that staff users refer to The Northern School of Art social networking guidelines, and students refer to guidance on safe use of the internet on the VLE. Furthermore, users should not transmit any information that may be damaging to the School or themselves.

x. Users accessing the Internet should not visit sites that violate the law. The School shall reserve the right to block access to any site it reasonably deems inappropriate and shall maintain logs of sites visited by all users that may be audited at any time. Users who need to use blocked sites for the purpose of study, should first obtain signed authorisation from their Senior Lecturer leader this can be done by completing the internet unblocking form (available on the School intranet or from IT), also the user should observe prudence in viewing the site and should take care that it will not cause offence to other users. As part of the content-filtering process, the School is allowed to provide caching services.

3.12 Wearable Technology

Wearable devices (e.g., smartwatches, fitness trackers, smart glasses, AR/VR headsets) may be used for productivity, health monitoring, and timekeeping if they do not disrupt work or study.

a. Devices must be on silent or vibrate during meetings, classes, exams, or professional activities.

b. Entertainment, gaming, or social media use is limited to breaks and lunch periods.

c. Devices must NOT be connected to the School’s network.

d. Storing, transmitting, or displaying sensitive organisational information on wearables is prohibited.

e. Recording (audio, video, photo) in private or confidential areas is forbidden, and recording individuals without consent is prohibited.

f. Wearables must be removed during exams and assessments; unauthorized possession may result in disciplinary action.

g. Breaches may lead to restricted access or other disciplinary measures.

Privacy and Security

3.13 The School must maintain security within its network but tries to do this without imposing restrictive regimes on the user. However, co-operation from users is essential to preserve security. Therefore, users must use the system in a manner which respects and preserves the privacy and rights of others. For example, users should not attempt to gain access to the files or directories of another user. Nor should users attempt to intercept any network communications such as electronic mail. Any breach of security should be communicated to the IT team or the IT Manager.

System Integrity

3.14 Users should not interfere with or alter the system integrity. Such actions include the impersonation of other people in communications, attempts to capture or crack passwords, attempts to decode encrypted information or any other form of interference with data and programs belonging to other users, and efforts to restrict or deny access to other legitimate users.

Intellectual Property Rights

3.15 Some software and data that reside on the computing systems are the intellectual property of particular users or third parties and are protected by copyright and other laws, together with licences and other contractual agreements. Users must abide by these restrictions, which may include prohibitions against copying, or against their use on unauthorised systems. Such restrictions are typically made known in comments at the beginning of the program or data or in statements in the accompanying documentation.

Using Your Account

3.16 You will have been allocated one or more accounts on computer systems in the School. These are for your personal use only. You should not disclose your password to others or allow anyone else to use your account. Anyone who has a valid reason for using the computers will be allocated his/her own account and should not use anyone else's. The simple exception to this rule is if a user is being instructed by another, e.g. a lecturer and student in a classroom situation or IT support and a user in a support call event. There are processes that allow staff to access other user's files under extreme circumstances and these can be negotiated with the coordination of the IT Manager, never be tempted to hand-over a password under any circumstance.

3.17 Under no circumstances should you tell anyone your password. If you really have to document your password, it must be kept under lock and key or a suitable encrypted password safe, never note it down on a piece of paper. It is the responsibility of each PC user to take all reasonable precautions to safeguard the computer and the

information on it. This includes logging out when the computer is not attended, and also protection from physical hazards such as liquids.

3.18 Special consideration should be given to the protection of portable devices including but not limited to laptops, tablets, phones, etc. as these are more open to theft and physical damage. If left unattended they should be kept under lock and key and under no circumstances should they be left in a vehicle. Caution should also be taken with storing sensitive data on a USB stick, digital removable media (CD, DVD, etc.) portable hard disk drive or any other portable device including laptops, tablets, smartphones, etc... Encryption should be employed on all sensitive portable data.

Unauthorised and Private Use

3.19 Use of the computers for commercial work is strictly forbidden unless special permission has been obtained. Permission can be sought through the Senior Management Team.

Offensive Material

3.20 It is strictly forbidden to transmit or store on School computer systems any material that is offensive. Offensive material is defined as any stored, published or broadcast content (such as articles, photographs, films, or websites etc.) that is likely to be upsetting, insulting, or objectionable to some or most people. Examples of offensive materials include pornography, any material designed to arouse hatred, bullying etc. It is the School policy that the transmission or storage of offensive material may constitute harassment. Harassment is unacceptable in the School whether it is unlawful and will be dealt with as gross misconduct under the disciplinary procedure. Some activities may constitute a criminal offence, and the police involvement may be necessary, the police have very considerable powers to investigate suspected cases.

Computer Publication

3.21 Computer users in the School have the ability to easily publish material in a variety of ways such as contributing to forums, posting on social network site, generally making documents available on the Internet, etc. This constitutes `publication' just as much as writing a letter to a newspaper or publishing a book. Computer publications can be seen to originate from the School (e.g. by Internet addresses which are automatically attached to the documents). Great care should be taken to ensure that all published material conforms to the high standards of the School. It is strictly forbidden to publish any material likely to bring the School into disrepute.

Email

3.22 Users must use their email responsibly. Be wary of unsolicited email especially those containing attachments or links. If there are hyperlinks in an email check the web address to ensure it is legitimate before clicking on as this can lead to a security breach (by phishing) and is the most common approach by hackers to enter a network. Never forward `chain letters' or send offensive messages to anyone. If you

receive offensive or abusive email, do not respond in kind and either report the incident to the IT Unit or ignore it completely. Email should never be sent to mailing lists (which often contain very large numbers of recipients) except when appropriate to do so. Please try to maintain a private email account in addition to your School one, using your private account for such things as banking, social networking, etc., remember that your School email account will not be available once you leave the School and some sites will distribute your email account details to spamming agents who can, in turn, lead to unnecessary email in your School account.

Disciplinary Action

3.23 Disciplinary action will be taken against any member of the School who infringes the regulations on computer usage. In serious cases of unauthorised access to computer systems or the theft of hardware/software or other intellectual property then it may constitute a criminal offence, and if so the police will be informed.

3.24 In all cases of violation of this policy, School disciplinary procedures will be followed. Please note that misuse of the School IT systems may be considered gross misconduct and result in summary dismissal for staff (without noticed or pay in lieu of notice) or immediate withdrawal from course or programme (students).

3.25 If agency staff or contractors violate this Policy, the matter will be reported to the appropriate agency or contractor to be dealt with under their procedures. The School may require the agency or contractor to provide an alternative worker and exclude the person suspected of violating the policy from the School premises. Alternatively, the contract of work with the agency or contractor may be cancelled.

Data Protection

3.26 Whilst using IT facilities are provided by the School, individuals must comply with all current data protection legislation that applies to the UK. Failure to do so could result in disciplinary action against that individual as part of the School's policies and procedures. An individual who shares their own data does so at their own risk. Any rights conferred by legislation concerning the usage and protection of your data still apply. For full information, please see the School's Data Protection Policy.

Surveillance

3.27 The School reserves the right to exercise control over all activities using its computer-related facilities, including examining the content of users' data and communications, for example stored/archived data, email, etc. and also observing a user's online activities in real-time, such as search engine enquiries, social media entries etc.

3.28 Examples of instances necessitating examination:

a. For the proper regulation of the School's facilities;

b. In connection with properly authorised investigations in relation to breaches or alleged breaches of provisions in the School's regulations.

c. To meet legal requirements.

d. To support the government's counter-terrorism prevent strategy

e. To safeguard staff and students

3.29 The School reserves the right to carry out monitoring exercises on its systems, possibly without prior notice. The School is committed to ensuring that any monitoring is undertaken with reference to the privacy of the user and with regard to the Data Protection Act, the Lawful Business Regulations and the Human Rights Act.

Equality impact statement

3.30 This procedure will be implemented in line with the principles of the School's commitment to equality and diversity which are: The Northern School of Art is committed to the principles of equality and diversity and aims to ensure that all employees and School users are treated fairly and equally regardless of age, disability, gender reassignment, marriage and civil partnership, pregnancy and maternity, race, religion or belief, sex, or sexual orientation.

Document Control – Including Archiving Arrangements

3.31 The Director of HE Quality and Enhancement is responsible for maintaining an index of policies and procedures in use and will act as an archivist. A single library of School policies and procedures will be maintained. Any policies and procedures that are replaced or are no longer active will be archived.

3.32 All 'live' policies and procedures will be accessible to staff and students in hard copy via policy and procedure files and will be published on the school's website and VLE.

3.33 The policy and procedure will be reviewed by the date shown on the front cover sheet, or sooner if a change in legislation, best practice, or other circumstances indicate that this is necessary. If for whatever reason, the policy and procedure are not reviewed by the date shown, the policy and procedure shall stay in force until formally reviewed.

4.0 IT CHANGE MANAGEMENT POLICY

4.1 Many of the processes and systems used by The Northern School of Art are underpinned by IT systems. Change is necessary to maintain and improve the IT facilities offered, to ensure the School is able to carry out its commitments and priorities of teaching, research and administration.

4.2 The IT Department provide a complex and interdependent set of services for the School. To ensure that maintenance work and improvements are completed without causing too much disruption to our users, IT manage changes to these systems in a controlled, planned and informed way; considering risks and any potential negative impact to staff and students.

Change Approval Process

4.3 IT follow a standard process to assess, approve and implement changes to services. This ensures:

- changes are well thought through
- adequately planned
- ready for implementation
- do not conflict with other planned work
- IT staff are available to carry out and support the change.

4.4 Depending on the scale of a change, it will either be classified as Minor, Significant or Major change.

4.5 The Systems Manager approves Minor changes on a daily basis, as these are low risk and unlikely to have an effect on School users even if they go wrong. Significant and Major changes are approved as and when required by the IT Manager and a Vice Principal through the Change Request form.

Testing of Significant or Major Changes

4.6 Minor changes with low impact are not heavily tested before roll out, however whenever possible all significant or major changes are tested in a test environment generally this is a handful of machines or servers. Once the test has shown to not cause any negative impact the changes are rolled out.

Training

4.7 Any changes that require training, will be rolled out only after the training has been planned and communicated to users at the appropriate time. This training can take the form of an email with a document or video attached with the training material, one to one training on a request basis, or training in groups done internally or externally.

Critical Periods

4.8 During critical periods in the academic year, such as enrolment, induction week and clearing the impact of an IT change going wrong could cause reputational or financial damage to the School.

4.9 To protect against this, IT reduces the number of changes we make, or even stop implementing changes completely. When we do this, we refer to either Change Exception Periods (when we limit changes made) or Change Freezes (when we stop implementing changes).

4.10 Our IT services continue to be available; however, changes to them will not be made unless they are needed in an emergency to keep IT facilities and services running.

5.0 IT USER ACCESS MANAGEMENT POLICY

Purpose

5.1 The purpose of this policy is to prevent unauthorised access to The Northern School of Art information systems. The policy describes the registration and de-registration process for all School information systems and services. These policies apply especially to new starters, leavers and those moving job, responsibility or Department. These policies should also be seen in the light of HR procedures to verify a new starter's qualifications, references and right to work in this country.

New Users

5.2 Access to The Northern School of Art information services is controlled via user accounts. Each user is identified by a unique user ID so that user access can be controlled and restricted according to their relevant area of operation and assigned rights.

5.3 New employee accounts are created by the Network Administrator following a formal notification from HR with details of the user's role and accountabilities. New student accounts are created by an automatic process initiated by their enrolment via the student management system (ProSolution) and they are assigned basic access rights appropriate to their function. A generic single use password is assigned to all new user accounts, thereafter the user is required to set a password of their choosing.

5.4 The use of generic IDs is only permitted where the user has not been assigned a User ID (i.e. visitors).

5.5 There is a standard level of access, other services can be accessed when specifically authorised by HR/line management.

5.6 A request for service must be made in writing (email or hard copy) by the user's line manager, by HR or by a senior lecturer in the case of a student. The request is free format, but must state:

- Name of person making request
- Job title of the newcomers and workgroup
- Start date
- Services required (default services are: MS Outlook, MS Office and Internet access)

5.7 The user signs the form indicating that they understand the conditions of access.

5.8 Access to all School systems is provided by IT and can only be started after proper procedures are completed. A new user will be set up on receipt of written notification but not made available, by issue of password, until the individual's start date. IT will maintain a record of all requests in the Helpdesk and will file email paper copies in the user access file.

Password Requirements

5.9 All staff must adhere to the enforced complex password policy when changing their password or for new staff creating a password for the first time. The password must be a minimum of 8 characters and must meet the complexity requirements detailed below.

Minimum length = 8 characters

Passwords must contain characters from three of the following four categories:

Uppercase characters of European languages (A through Z)

Lowercase characters of European languages (a through z)

Base 10 digits (0 through 9)

Nonalphanumeric characters: ~!@#$%^&*_-+=`|\(){}[]:;"'<>,.?/

Change of password

5.10 Where a user has forgotten his/her password, the helpdesk is authorised to issue a replacement. Upon receipt of such a request the Helpdesk will

1. Ensure the request is logged.

2. Confirm the identity of the user by checking their ID card or referring to a stored photo for the individual.

3. Issue a temporary, single use, password which will require the user to set up a formal password.

Removal of users

5.11 As soon as an individual leaves the School's employment, all his/her system logons must be revoked. As part of the employee termination process HR (or Student Administration in the case of students) will inform IT of all leavers and their date of leaving. All notifications will be stored in the Helpdesk. Additionally, IT will positively confirm employee leavers with HR, each Month, retaining a copy of the e-mail creating a Helpdesk. Unless otherwise advised, IT operations will delete network access for all leavers as late as possible on the leavers last day (old user ID's are removed and not re-issued). This will include access to all network services. IT will not immediately delete all leaver files, but may move leavers files to cold or archive storage if required for operational reasons. Normally a leaver's data will be left in its existing directory for one month and then archived. Files can be recovered if required.

Privilege management

5.12 "Special privileges" are those allowed to the IT Management, allowing access to sensitive area (for example, Finance, HR etc). For non-IT staff to be granted additional access to network resources, either a request needs to be made by email

or filling in the Additional Account Privileges Request Form. If done via email IT will seek approval from the appropriate manager of that resource.

Review of user access rights

5.13 The Systems Development Manager will conduct a review of all network access rights at least twice a year, which is designed to positively confirm all users. Any lapsed or unwanted logons, which are identified, will be disabled immediately and will be deleted unless positively reconfirmed. Annually the Systems Development Manager will also conduct a review of access to applications. This will be done in cooperation with the application owner and will be designed to positively re-confirm all users. All other logons will be deleted.

6.0 ONLINE SAFETY POLICY

Introduction

6.1 The Northern School of Art is committed to online safety as part of its overall safeguarding strategy and expects all staff and students to share this commitment.

This Policy outlines the measures in place to protect the School community from online harm and to promote a secure digital environment across the four components outlined in Keeping Children Safe in Education:

a. Content - being exposed to illegal, inappropriate, or harmful content, for example: pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation, and extremism;

b. Contact - being subjected to harmful online interaction with other users; for example: peer to peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes;

c. Conduct - online behaviour that increases the likelihood of, or causes, harm; for example, making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography, sharing other explicit images and online bullying, and

d. Commerce: risks such as online gambling, inappropriate advertising, phishing and or financial scams.

6.2 This Policy and the associated procedure also take into account the following guidance and legislation:

a. Sharing nudes and semi-nudes: advice for education settings working with children and young people 2024 (UK Council for Internet Safety)

b. Searching, Screening and Confiscation - non statutory advice (DfE)

c. Prevent Duty guidance: England and Wales (2023)

d. Ofsted's Inspection Framework

e. Data Protection Act (2018)

f. Education Act (2002)

6.3 The objectives of this Policy are:

a. to safeguard students, staff and visitors from online threats

b. To promote responsible and ethical use of digital resources

c. To ensure compliance with legal and regulatory requirements

d. To educate the School community about online safety practices

Scope

6.4 This Policy is applicable to the entire School, staff students and visitors and is part of our commitment to safeguard all members of its community. It covers incidents that take place within the School and also online activities that may take place outside of the School but relate to the School's reputation or safety of its students and/or staff.

6.5 This Policy relates to all actions taken to ensure staff and students are safe online and all types of activities that have the potential to harm young people, such as online bullying, grooming, sexting, etc.

Definitions

6.6 For the purposes of this Policy the term "**child**" or "**children**" refers to a person or persons under the age of 18 years (as defined in the Children Act, 1989).

6.7 A **vulnerable adult** refers to any person up to the age of 25 who is considered at more risk than others of that age, for example, those in receipt of an Educational Health Care Plan.

6.8 The term "**safeguarding**" relates to the action taken to keep young people and vulnerable adults safe from the risk of harm and the action taken to promote their welfare in order that they can thrive and reach their potential.

6.9 **Bullying** - repetitive, intentional hurting of one person or group by another person or group, where the relationship involves an imbalance of power. Bullying can be physical, verbal or psychological. It can happen face-to-face or online.

6.10 **Harassment** is a broad term that refers to unwelcome and inappropriate actions, behaviour, or comments directed at an individual or group that cause distress, discomfort, or harm. It can take many forms, including but not limited to verbal, physical, sexual, cyber and psychological

6.11 **Extremism** is the promotion or advancement of an ideology based on violence, hatred or intolerance, that aims to:

a. negate or destroy the fundamental rights and freedoms of others; or

b. undermine, overturn or replace the UK's system of liberal parliamentary democracy and democratic rights; or

c. intentionally create a permissive environment for others to achieve the results in (1) or (2).

6.12 **Radicalisation** is the process by which a person is drawn into extreme views in support of extreme ideologies or beliefs, terrorist groups and activities.

6.13 **Youth Produced Sexual Imagery or sharing nudes or semi-nudes** – this refers to the sending or posting of nude or semi-nude images, videos, or live streams by young

people under ethe age of 18 online. This could be via social media, gaming platforms, chat apps or forums. It could also involve sharing between devices via services such as Apple's AirDrop which works offline. The sharing of images can happen publicly, online, in one-to-one messages or via group chats and closed social media accounts. Alternative terms used may be 'dick pics', 'pics', 'indecent imagery' or 'sexting'.

POLICY

6.14 All reasonable precautions will be taken to prevent access to inappropriate material within the School, 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 a computer connected to the School network. The School cannot accept liability for any material accessed, or any consequences of Internet access.

6.15 The School actively encourages students to use their own devices for purposes of research or visual inspiration. Many students have unlimited and unrestricted access to the internet via mobile data (i.e. 3G, 4G and 5G). These devices are not governed by the School's infrastructure and can bypass any and all security and filtering measures that are or could be deployed. Mobile device access to the internet will be filtered when it is done through the School's wireless networks, however access using a mobile data service cannot be monitored. The School is therefore committed to ensuring students and staff are educated with regards to appropriate use of such technology through training and awareness activity.

6.16 The promotion of online safety within IT activities is to be considered essential for meeting the learning and development needs of students. The School will help students to understand the risks posed by individuals who use the internet and social media to bully, groom, abuse or radicalise other people, especially children, young people and vulnerable adults.

6.17 School staff will need to be continually alert to any suspicious activity involving computers and the Internet and will be provided with appropriate training and awareness to enable them to do this effectively.

6.18 Staff will receive regular updates regarding Online Safety through a variety of mediums such as awareness sessions, updates within the staff newsletter and via the Safeguarding Committee.

6.19 Access to the Internet and e-mail is provided to support the curriculum, School administration and for staff professional development only. Recreational or personal use of the Internet and e-mail system is not encouraged. All staff and students must read and confirm by accepting an online form that they have read the "Acceptable Use Policy" before using any School IT resource. Access to systems should be made by authorised passwords, which must not be made available to any other person.

6.20 Any person not directly employed by the School will not automatically be provided with access to any of the School systems with the exception of filtered Wi-Fi access.

Access will be allowed only after consideration of the individual and the circumstances of operation, generally under the advice of the IT Department.

6.21 Methods to identify, assess and minimise risks will be reviewed regularly by both the IT Department and the Safeguarding Committee.

6.22 This policy informs and supports a number of other School policies, including our Staff and Student Code of Conduct, IT Acceptable Use Policy, Student Harassment and Bullying Policy, Staff Harassment & Bullying Policy, Sexual Harassment Policy, Prevent Policy and the School's Safeguarding Policy and Procedure. It is recommended that it is read in conjunction with these related policies and procedures.

Roles and Responsibilities

6.23 **Governors** are responsible for ensuring that that are relevant policies in place and a mechanism to support staff and students.

6.24 The School has a member of the Governing Body with responsibility for online safety as part of their role as **Safeguarding Governor**. As part of this role they will:

- discuss online safety issues with the Designated Safeguarding Lead as part of the School's governor 'buddy' approach;
- discuss and raise online safety concerns at the Safeguarding Committee;
- report to the Governors on online safety issues and actions and keep them up to date with current thinking and good practice.

6.25 **The Principal** - The Principal has a duty of care for ensuring the safety (including online safety) of members of the School community.

6.26 **Designated Safeguarding Lead and Deputy Designated Safeguarding Leads** (DSL & DDSL) - will work alongside the IT Manager in all matters regarding safeguarding and online safety. They will be trained in online safety issues and be aware of the potential for safeguarding issues to arise from access to illegal and/or inappropriate materials, inappropriate on-line contact with adults or strangers, potential or actual incidents of grooming and online bullying.

Their role will include:

- ensuring all appropriate staff receive the appropriate training, guidance, time and resources to effectively implement online safety policies and procedures;
- leading on the School's strategic approach to online safety;
- ensuring allegations of misuse or known incidents are dealt with appropriately and promptly, in line with safeguarding and disciplinary procedures, and in liaison with other agencies, where applicable.

- Liaise with the **Learning Technologist** to ensure students receive sufficient information to keep themselves safe online.

6.27 **IT Manager** - Has responsibility for ensuring:

- that the School's technical infrastructure is secure and is not open to misuse or malicious attack;
- that the School meets required online safety technical requirements;
- that users may only access the networks and devices through a properly enforced password protection policy;
- filtering is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person;
- that they keep up to date with online safety technical information in order to effectively carry out their online safety role and to inform and update others as relevant;
- that the use of the network / internet / Virtual Learning Environment / remote access / email is regularly monitored in order that any misuse or attempted misuse can be reported to a Safeguarding Lead;
- that monitoring software / systems are implemented and regularly updated.

6.28 **Teaching and Support Staff** – must ensure that:

- they have an up to date awareness of online safety matters and of the current School online safety policy and practices;
- thy report any suspected misuse or problem to a Safeguarding Lead;
- they maintain all digital communications with students on a professional level and only carry them out using official School systems;
- they embed online safety issues in aspects of the curriculum and other activities;
- students understand and follow the online safety and acceptable use policies;
- they monitor the use of digital technologies, mobile devices, cameras etc. in sessions and other School activities and implement current policies with regard to these devices.

6.29 **Students** should ensure they:

- use the School digital technology systems in accordance with this policy and the IT Acceptable Use Policy;
- understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so;

- understand the importance of adopting good online safety practice when using digital technologies out of School and realise that the School's Online Policy covers their actions out of School, if related to their membership of the School.

Filtering and Monitoring

6.30 The School ensures a safe and secure online environment by implementing effective filtering and monitoring systems that protect against inappropriate content, conduct and online threats

6.31 The School's firewall, with built in web filter, is supplied and managed by Smoothwall, a digital safety technology provider that has over 2 decades of experience in supporting UK education providers

6.32 The firewall protects the School's computer systems from unauthorised access or anyone attempting to infiltrate the School's network

6.33 The web filter is an automated system that will block access to any inappropriate websites. What is deemed as inappropriate is reviewed and added to on a regular basis by Smoothwall, but includes such things as access to explicit content, academic dishonesty, gambling, terrorism, weapons. The level of filtering varies from HE to FE, reflecting the differing needs and ages of the students on each site

6.34 The School utilises Smoothwall's Managed Monitoring System to identify any concerning behaviour online and alert safeguarding staff so that they can take appropriate action to safeguard staff and students. The MMS service provides a 24/7 online digital monitoring service, using advanced technology and trained human moderators who will then contact staff within the School by an email alert or a phone call, depending on the severity and urgency of the content detected

6.35 The filtering and monitoring systems also support the School's approach to Prevent by raising alerts of any activity related to

a. the radicalisation of individuals;

b. the promotion of terrorism;

c. the normalising abnormal views and behaviours, such as extreme ideological views or the use of violence to solve problems and address grievances.

6.36 All content being monitoring will be reviewed by designated School staff on an annual basis to ensure it reflects local need and risk and it is also continually updated by Smoothwall in terms of keywords that are monitored and flagged

6.37 Testing of both the filtering and monitoring systems is completed by the IT department on a monthly basis. Testing of the monitoring system is completed in conjunction with HR and Student Services. Testing of the filtering service is completed using the South West Grid for Learning's (SWGfL) testing tool. This checks that the filtering system is blocking access to

a. Illegal child sexual abuse material;

b. Unlawful terrorist content;

c. Adult content.

6.38 Staff monitoring is limited to Prevent and health (suicide risk)

6.39 A record of these tests is maintained and presented in the IT update report at the Safeguarding Committee

6.40 By incorporating robust filtering and monitoring measures, the School aims to create a secure online environment that protects all users from inappropriate content and online threats

Access

6.41 Any person not directly employed by the School will not automatically be provided with access to any of the School systems with the exception of filtered Wi-Fi access. Access will be allowed only after consideration of the individual and the circumstances of operation, generally under the advice of the IT Department

6.42 Access to the Internet and e-mail is provided to support the curriculum, School administration and for staff professional development only. Recreational or personal use of the Internet and e-mail system is not encouraged. All staff and students must read and confirm by accepting an online form that they have read the “Acceptable Use Policy” before using any School IT resource

6.43 Access to systems is by authorised passwords, which must not be made available to any other person

6.44 Most students have their own smart phones, tablets or laptops. Students are encouraged to use these on the School’s password filtered Wi-fi network for added protection

6.45 All reasonable precautions will be taken to prevent access to inappropriate material within the School, 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 a computer connected to the School network. The School cannot accept liability for any material accessed, or any consequences of Internet access

6.46 The School actively encourages students to use their own devices for purposes of research or visual inspiration. Many students have unlimited and unrestricted access to the internet via mobile data (i.e. 3G, 4G and 5G). These devices are not governed by the School’s infrastructure and can bypass any and all security and filtering measures that are or could be deployed. Mobile device access to the internet will be filtered when it is done through the School’s wireless networks, however access using a mobile data service cannot be monitored. The School is therefore committed to

ensuring students and staff are educated with regards to appropriate use of such technology through training and awareness activity

Staff and Student Awareness

6.47 The School is committed to ensuring staff and students are well-informed about online safety practices and understand the importance of protecting their personal information and digital footprint. This will be achieved by education on:

a. Understanding Online Risks

i. Educating about recognising phishing emails and scams;

ii. Raising awareness about the impact of cyberbullying, encouraging students to report any incidents and ensuring staff are aware of the signs of cyber bullying and know what steps to take in addressing any incidents with students;

iii. Highlighting the importance of keeping personal information private and being cautious about what they share online;

iv. Ensuring staff are aware of the importance of safeguarding student information and being cautious about sharing sensitive data online;

v. Supporting staff and students to understand and recognise the risks posed by individuals who use the internet and social media to groom, abuse or radicalise other people;

vi. Educating and reminding students about the risks posed by posting images online

b. Safe Online Practices:

i. Encouraging the use of strong, unique passwords for different accounts and the importance of regularly updating them;

ii. Promoting the use of two-factor authentication (2FA) to add an extra layer of security to online accounts;

iii. Advising use of secure, encrypted connections (HTTPS) when browsing the internet, especially when accessing sensitive information.

c. Social Media Awareness:

i. Education on how to adjust privacy settings on social media platforms to control who can see posts and personal information;

ii. Making students aware that their online actions can have long-term consequences and encourage them to think before they post;

iii. Encouraging staff to maintain professional conduct online and be mindful of their digital footprint.

d. Reporting and Support:

i. Providing clear instructions on how to report online safety incidents, including cyberbullying, harassment, and suspicious activities;

ii. Informing about available support resources, such as counselling services, IT support and online safety workshops.

e. Continuous Education:

i. Organising regular workshops and seminars on online safety to keep students updated on the latest threats and best practices;

ii. Providing access to online resources, such as articles, videos, and tutorials, to help staff students stay informed about online safety.

f. Collaboration and Communication:

i. Encouraging staff to collaborate and share best practices for online safety within their teams;

ii. Fostering an environment of open communication where staff and students feel comfortable discussing online safety concerns and seeking advice.

6.48 Key staff, such as Safeguarding Officers and those responsible for advising on safeguarding matters relating to IT, will also maintain up to date knowledge of trends and online concerns by regular continuous professional development and attendance at networking events such as those organised by the local Digital Resilience Group

6.49 By ensuring staff are well-informed and proactive about online safety, and fostering a culture of awareness and proactive behaviour, the School aims to create a safe and secure online environment for both staff and students

Radicalisation and the use of social media to encourage extremism

6.50 The School does not condone any form of extremism or radicalisation

6.51 Reducing the presence of extremist groups online is the responsibility of all School staff and as part of the PREVENT duty and Keeping Children Safe in Education all staff have a responsibility to report the presence of extremist material online

Sensitive or extremist related research

6.52 Research involving sensitive or extremist-related topics requires careful consideration to ensure the safety and integrity of both the student or staff member and of the institution

6.53 Staff members undertaking any such research will seek guidance from their Line Manager. Students need to seek prior approval from their teaching staff before commencing research on topics of this kind. Consultation with the DSL is required, when necessary, to ensure that the research is ethical, complies with relevant legal requirements and that any associated risks are understood

Online bullying / cyber bullying

6.54 The School does not condone any form of bullying or harassment which include that online

6.55 Any student carrying out bullying or harassment online will be subject to the School's Disciplinary Procedure

IT based sexual abuse

6.56 It is recognised that the impact on a young person of IT based sexual abuse is similar to that for all sexually abused students, with the additional dimension of there being a record of the abuse

6.57 Staff will support and take a trauma-based approach to any student affected by IT based sexual abuse, working with outside organisations to ensure specialist support is in place, and recognising that IT based sexual abuse of a child constitutes significant harm through sexual and emotional abuse

Youth produced sexual imagery

6.58 All incidents of youth produced sexual imagery (YPSI) will be dealt with as a safeguarding concern

6.59 It is recognised that young people who share sexual imagery of themselves or their peers are breaking the law, however the importance of avoiding criminalising of young people unnecessarily is recognised. The School will therefore work in partnership with external agencies with a view to responding proportionately to the circumstances of any incident

6.60 The primary concern at all times will be the welfare and protection of the young people involved

Taking and storing images of staff and students

6.61 The taking and storing of images of staff and students for institutional purposes is only permitted with expressed permission

6.62 The taking of photographs with devices such as mobile phones, tablets, or cameras by other students or staff without the expressed permission of the person being photographed is strictly forbidden in the School

Issues relating to online safety

6.63 School staff will need to be continually alert to any suspicious activity involving computers and the Internet and will be provided with appropriate training and awareness to enable them to do this effectively

Monitoring and evaluation

6.64 The DSL and the IT Manager have joint responsibility for reviewing and updating this Policy for approval by the Safeguarding Committee on an annual basis

6.65 Issues of online safety raised will be reported on and considered in the Safeguarding Committee meetings held regularly throughout the academic year.

7.0 ONLINE SAFETY PROCEDURE

7.1 All users of the School IT systems are made aware of the IT Acceptable Use Policy which outlines the rules and guidelines around the safe use of the School's IT systems in order to protect and safeguard both the systems and the users. Students are made aware of the Policy during enrolment and staff at appointment. Staff and students must each agree on acceptance to allow access to the institution's IT facilities.

Reporting of Online Safety / Safeguarding issues and concerns

7.2 Online **safety** concerns include phishing and scam emails, malware and viruses, identity theft, online scams, and data breaches

7.3 Any online **safety** concerns should be brought to the attention of the IT Manager. In the event of a data breach the Data Protection Officer should also be informed.

7.4 Online **safeguarding** concerns include exposure to harmful or inappropriate content (for example, sexual, extremist, promoting self-harm or suicide), cyber-bullying, harassment, sexting, grooming)

7.5 In the event of a concern relating to any of the above online activity staff should refer to the Safeguarding Procedure and follow the general procedure for reporting serious concerns. Students can raise any concerns with a member of staff who will then pass this on to a Safeguarding Officer

Monitoring Alerts

7.6 Concerns raised through the School's monitoring system (Smoothwall's Managed Monitoring System) are automatically directed by email to either the Vice Principal – People Services or to Student Services depending on whether the alert has been triggered by a member of staff or a student. Any alerts that cannot be identified as either staff or student are sent to the Vice Principal – People Services and if found to be a student, sent to Student Services.

7.7 The Vice Principal – People Services / Student Services will then evaluate whether a discussion is needed with the member of staff or student or the student's tutors to ensure that a safeguarding issue is either dealt with, support offered or to investigate why the alert has been triggered

7.8 The Students Services Team are responsible for keeping records of all alerts relating to students which should include a clear and comprehensive summary of what the alert is relating to and how it was followed up and resolved

7.9 The HR Department will keep a record of all staff alerts and actions taken

Concerns relating to radicalisation and extremism

7.10 All staff have a responsibility to be vigilant of any online activities related to radicalisation and extremism. It is essential for staff to note that students may be researching for current subjects of education and academic themed projects therefore must check research topics to prevent misguided identification of individuals whom may be only engaged in academic research only

7.11 Any student wishing to research potentially extremist related subjects or subjects linked to terrorism should advise teaching staff prior to conducting any online research so that they can be appropriately supported. The Designated Safeguarding Lead (DSL) should also be informed

7.12 If staff observe through a link, or click on a webpage, containing extremist material of any kind the steps below should be followed:

a. Take a screenshot of the page using the print screen button on your keyboard

b. Go to your email account and right click on the main body of a new email

c. Go to paste options and paste the image into the email

d. Send the email to the Designated Safeguarding Lead and IT Manager advising what has happened

e. Return to the webpage and highlight the URL address and right click and copy

f. Navigate the browser away from the site to the Counter Terrorism Internet Referral Unit https://www.gov.uk/report-terrorism (the URL from the offending website needs to be ready to submit at this point).

7.13 If staff observe a student with an open screen with potentially extremist material they should report it to DSL with the following information:

a. computer number

b. date and time

c. person using the computer at the time

d. a description of what was observed

7.14 The IT Manager will then obtain the URL data from the system for inspection and refer these to a Safeguarding Officer to consider if a PREVENT referral is necessary. The DSL should be informed

7.15 Periodically IT staff, when conducting IT reviews of school computers may identify devices where extremist material has been accessed, this may have occurred inadvertently or purposefully by the user. In this event staff should take a note of the

device number, all user details (if the device has been used by more than one individual) and a description/screenshots and URL. This should then be passed onto the IT Manager and DSL for reporting to the Police

7.16 Once identified that there is extremist material on a device all access to the device must be prohibited as this may form part of a police investigation and should be quarantined securely and appropriately until notified by police that the device is no longer required

Audit of IT systems and resources

7.17 Testing of both the filtering and monitoring systems is completed by the IT Systems Development Manger on a monthly basis

7.18 The content being monitoring will be reviewed by the IT Manager and the DSL on an annual basis to ensure it reflects local need and risk and it is also continually updated by the service provider in terms of keywords that are monitored and flagged

7.19 An annual IT risk assessment will be completed to highlight any areas for concern and any actions needed

7.20 All of the above will be reported on in the School's Safeguarding Committee

IT based sexual abuse

7.21 Victims of IT based sexual abuse should:

a. report to a member of staff or HR as soon as possible

b. save all relevant communications, screenshots, and any other digital evidence

c. access counselling services provided by the School for emotional and psychological support

7.22 Upon receiving a report of IT-based sexual abuse, the School will:

a. initiate an investigation within 24 hours of receiving the report

b. report to and work with external authorities and organisations, as appropriate

c. ensure the privacy of all parties involved during the investigation process

d. if the perpetrator is a member of the School community, apply appropriate disciplinary measures against them, which may include suspension or expulsion or dismissal

7.23 Relevant staff working with a student that has been affected will be informed to enable a trauma-based approach to be taken and relevant support and understanding is adopted. They will also be alerted to the possibility that:

a. images may have been distributed on the internet or by mobile telephone

b. an adult or older child may be involved in grooming a child for sexual abuse, including making abusive images

c. an adult or older child may be viewing and downloading child sexual abuse images

Taking and storing images of students

7.24 Prior to taking any photos or images of students, staff must check whether students have explicitly not given this consent at enrolment.

7.25 Staff must ensure that photographs and images are only be used for the purpose intended, individual rights are respected that images conform to appropriate standards of integrity and decency

7.26 Wherever possible, staff should not photograph students using their own devices but should use School cameras, tablets or mobile phones. Staff using their personal phones to photograph students at School events must download the images onto the appropriate School drive and then delete them from their own devices

Youth produced sexual imagery

7.27 The types of incidents referred to in this section include where:

a. a person under the age of 18 creates and shares nudes and semi-nudes of themselves with someone they believe to be under the age of 18

b. a person under the age of 18 shares nudes and semi-nudes created by another person under the age of 18 with a peer under the age of 18

c. a person under the age of 18 is in possession of nudes and semi nudes created by another person under the age of 18

7.28 If staff become aware of an incident involving youth produced sexual imagery (YPSI) the following guidelines should be followed:

a. **Never** view, copy, print, share, store or save the imagery yourself, or ask the student to share or download – this is **illegal**

b. If you have already viewed the imagery by accident (e.g. if someone has shown it to you before you could stop them), report this to the DSL (or equivalent) and seek support

c. Do not delete the imagery or ask the young person to delete it

d. Do not ask the child/children or young person(s) who are involved in the incident to disclose information regarding the imagery. This is the responsibility of the DSL (or equivalent)

e. Do not share information about the incident with other members of staff, the young person(s) it involves or their, or other, parents and/or carers

f. Do not say or do anything to blame or shame any young people involved

g. Do explain you need to report it and reassure them that they will receive support and help from the DSL (or equivalent)

7.29 All incidents of YPSI should be reported to the DSL. Staff will not make their own judgements about whether an issue relating to YPSI is more or less serious enough to warrant a report

7.30 If staff become concerned about a YPSI issue in relation to a device in the possession of a student (e.g. mobile phone, tablet, digital camera), the member of staff will secure the device (i.e. it should be confiscated)

7.31 Staff **must not** look at or print any indecent images. The confiscated device will be passed immediately to the DSL, who will discuss the concerns with appropriate staff and speak to young people involved as appropriate

7.32 Further details relating to searching a student (if required) and confiscating devices can be found in the Safeguarding Policy and Procedure

7.33 Parents/carers of students will be informed at an early stage and involved in the process unless there is good reason to believe that involving parents would put the young person at risk of harm

7.34 The DSL should **not** view youth produced sexual imagery unless there is good and clear reason to do so. Wherever possible, the DSL's responses to incidents will be based on what they have been told about the content of the imagery

7.35 Any decision to view imagery will be based on the DSL's professional judgement. Imagery will never be viewed if the act of viewing will cause significant distress or harm to a pupil

7.36 In taking a decision to view any imagery the DSL should be satisfied that viewing:

a. is the only way to make a decision about whether to involve other agencies (i.e. it is not possible to establish the facts from the young people involved)

b. is necessary to report the image to a website, app or suitable reporting agency to have it taken down, or to support the young person or parent in making a report

c. is unavoidable because a young person has presented an image directly to a staff member or the imagery has been found on a School device or network

7.37 If considered necessary to view the imagery then the DSL will:

a. discuss the decision with the Principal

b. ensure viewing is undertaken by the DSL with delegated authority from the Principal

c. ensure viewing takes place with another member of staff present in the room, ideally the Principal, another Safeguarding Lead or a member of the senior leadership team. The other staff member does not need to view the images

d. wherever possible ensure viewing takes place on School premises, ideally in the principal or DSL's office

e. never copy, print or share the imagery: this is illegal

f. ensure wherever possible that images are viewed by a staff member of the same sex as the young person in the imagery

g. record the viewing of the imagery in the student's safeguarding record, including who was present, why the image was viewed and any subsequent actions; and ensure this is signed and dated and meets the wider standards set out by Ofsted for recording safeguarding incidents

7.38 If the School has decided that other agencies do not need to be involved, then consideration will be given to deleting imagery from devices and online services to limit any further sharing of the imagery

7.39 The DSL will make a judgement about whether a reported YPSI incident is experimental or aggravated (i.e. involves criminal or abusive elements beyond the creation, sending or possession of sexual images created by young people)

7.40 Aggravated incidents or where there is any concern that a young person has been harmed or is at risk of harm a referral will be made to Children's Social Care and/or the Police via the usual Safeguarding procedures. The Police will always be informed when there is reason to believe that indecent images involve sexual acts and any child in the imagery is under 13 years of age

7.41 Students involved with YPSI will be offered further support from Student Services to understand motivations behind sharing any images and / or help them navigate the wider implications and pressures that may now have to be faced

7.42 All incidents of YPSI will be recorded as a safeguarding concern

Monitoring and review

7.43 The IT Manager and Designated Safeguarding Lead have responsibility for reviewing and updating this Procedure

7.44 The IT Manager and Designated Safeguarding Lead will evaluate the effectiveness of the Procedure by using data collected and records of outcomes

7.45 Issues of online safety raised will be reported on and considered in the Safeguarding Committee meetings held regularly throughout the academic year

Related policies and procedures

a. Student Behaviour Policy
b. Safeguarding Policy and Procedure
c. Staff Code of Conduct
d. Student Code of Conduct
e. IT Acceptable Use Policy
f. Student Disciplinary Procedure
g. Student Behaviour Policy

8.0 MANAGEMENT OF PUBLIC INFORMATION PROCEDURE

Introduction

8.1 This procedure identifies the range of public information the Institution is responsible for publishing, the main channels used to communicate this, staff responsibilities and arrangements for assuring the accuracy and completeness on issue and whilst it remains in the public domain.

Scope

8.2 The Institution has responsibility for publishing a variety of public information materials relating to both staff and students which includes the following:

Marketing materials:

Course and programme Information that will help a potential student, parent, practitioner or employer decide to engage with the Institution. These have to meet, where relevant, the Institution's corporate guidelines, the requirements of the Awarding Body and need to accurately and completely reflect the Institution's provision.

Course/programme Information:

Information used by students to initiate enquiries and/or applications to Institution courses or programmes. This has to be accurate and complete to ensure students apply for the correct course or programme and are fully aware of any associated conditions and financial information that will impact upon their studies.

Student Services Information:

This may be used externally or internally to inform potential, and current students, and alumni. This has to accurately reflect the Institution offer and range of resources available, to ensure that expectations raised are realistically met.

Delivery and Support Material/Resources:

Detailed internal information available only to current enrolled student cohorts which is used to deliver the learning journey from enrolment through to exit covering:

- Programme or course information
- Timetables
- Academic regulations
- Student entitlement
- Module/unit details
- Assignments
- Handouts and other learning materials

- Information on Institution support services and facilities generally available to students
- N.B. Arts University Bournemouth has responsibility for publishing details regarding awards, grades and progression for their qualifications but the Institution takes responsibility for the initial provision of information and the checking of grades prior to Module and Awards Boards and before publication.

Institution Policies and Procedures:

These are published online to support institution compliance with policies.

Exclusions

8.3 The Institution is not responsible for public information outside of its control, for example:

- Information posted to Blogs used to support student learning
- Information on linked websites or sub/micro sites not controlled by the Institution

8.4 The Institution also publishes a wide range of information for individual students to maximise their quality of learning opportunities and help them engage with their learning from application, on programme/course through to their leaving. This is confidential information and can only be seen by individual students and staff. This is not deemed to be part of the Institution's public information policy.

Procedure

Key Channels of the Institution's Public Information

8.5 The table below indicates the main forms of material for the communication of public information. The Institution has assigned responsibility to named staff for the final approval of documentation, following checking processes, prior to publication. These staff are listed in the table below, which also lists the processes for the management and creation of the content.

Type of Information	Process/Responsibility
Institution Prospectus:	Overall approval of Principal, following checking by relevant staff

Type of Information	Process/Responsibility
Institution external information including website	The boxes below indicate who has responsibility for creating and checking the content which is communicated externally. The Marketing Team are to be the conduit for the posting of all external information
Curriculum Information	Individual Course/Programme Information checked and approved by Course/Faculty Leaders/Senior Lecturers Final sign off by relevant Vice Principal
Personnel Information	Vice Principal (People Services)
Student Services	Student Services Manager
Financial Information	Vice Principal - Resources
General Information	Head of Governance
Governor Information	The Head of Governance as set out in the Instruments and Articles which lays down what the Board should make publicly available with regard to the agenda and minutes of its meetings – the Institution has chosen to do this via a governor's website which the Head of Governance controls.
Information for Business	Marketing Team
UCAS website - course information	Head of Marketing and Recruitment based on programme information provided for prospectus and website by programme and course management.
Institution Social Networking Sites e.g. Facebook, Twitter	Moderated by Marketing Team
Marketing Materials tiers 14/Publicity	Marketing Team following flow chart process Examples of publications tiers 1 – 4 responsible for (appendix 3)
Additional external literature not outlined in appendix 4	Final approval by Principal to ensure that publicity meets Institution branding guidelines and messaging. Where necessary guidance sought from Marketing Team

Type of Information	Process/Responsibility
Show Materials	Final approval Head of Marketing and Recruitment following consultation with relevant Show Committee
Application information eg. Entry criteria/ How to apply	Head of Marketing and Recruitment
Curricula Information	Cluster Leaders (FE) Faculty Leaders/Senior Lecturers (HE)
Personnel Information	Vice Principal – People Services
Quality Documentation, Policies and Procedures	Checked by HE Director Quality & Enhancement / FE Quality Manager
Financial Information including fees, waivers and bursaries	Vice Principal - Resources
Corporation Board	Head of Governance
Student Handbook	• Contents approved during validation processes. • Updated annually to include variance to information provided by the Awarding Institution. • Approved following annual handbook updating day by Cluster Leaders and Faculty Leaders. • General Information concerning Student Services to be approved by Student Services Manager
Academic Curriculum areas	• Content approved prior to start of academic year by Faculty Leaders/Senior Lecturers. (HE) • Spot check throughout year by Cluster leaders (FE)
Assignment Briefs	• Verified by Faculty Leader or VP HE • Documented spot checks throughout year by HE Quality Operations Manager
Handouts, Learning Materials	• Created by module leader • Approved by senior lecturer.

Type of Information	Process/Responsibility
Awards and Progression	• Information regarding module grades issued by the relevant awarding body • Checked to ensure all appropriate students are listed and then distributed to Senior Lecturers by Academic Services for input of grades • Grades returned to Academic Services who then checks to ensure all grades have been submitted – this is the returned to the relevant awarding body who have responsibility for the production of module marks for module and awards Boards • Academic Services sends module packs to Senior Lecturers for checking to ensure grades are correct • Academic Services attends Module & Awards Board to record decisions
FE Academic Handbook	• Approved by Vice Principal FE
Course Handbook	• Approved by Course Leader
Unit Guides	• UAL Guides pre-written by awarding body • Units selected on an annual basis from a bank of units by Vice Principal FE and Course Leaders
Virtual Learning Environment (VLE) academic content	• Content approved prior to start of academic year by Course Leaders
Assignment Briefs	• Course Leaders have responsibility for creating briefs • Verified by Internal Verifier and sign off by Lead Internal Verifier
Handouts, Learning Materials	Approved by Course Leader
Financial Support	Approved by Student Services Manager
Disability Support	Approved by Student Services Manager
General Student Support e.g. accommodation	Approved by Student Services Manager

Type of Information	Process/Responsibility
Counselling	Approved by Student Services Manager

Roles and Responsibilities

Staff Responsibilities

8.6 Responsibility for the verification of public information has been assigned to the Senior Managers within the Institution, who are the content owners as set out in the procedure table. This is to ensure accuracy and completeness of information within each of the departments:

- FE and HE Academic Teams
- Registry
- FE and HE Quality
- Student Services
- Finance
- Marketing

Main External Forms of Information

8.7 It is recognised that some of the public information comes from a wide range of departments, particularly in relation to student recruitment notably the prospectus and website. In the case of these two publications the Marketing and PR Manager has responsibility for co-ordinating the information and ensuring that it has been signed off by the appropriate content owners prior to publication as indicated in the procedural table.

8.8 A draft copy of the prospectus is circulated to relevant Vice Principals, and relevant sections sent to Senior Lecturers, Arts University Bournemouth (HE only) where relevant, for final accuracy, completeness checks and sign off before issue for printing and final distribution.

Internal Information for Students

Curriculum Information

8.9 The cluster leaders/ Vice Principal FE take overall responsibility for the publication of curriculum data related to the prospectus, website and student handbooks.

8.10 Responsibility for the creation of course/programme information is devolved to Course/ Faculty Leaders but with some verification (outside the programme) taking place in respect to assignment briefs and marks.

8.11 The checking of content on the Virtual Learning Environment is the responsibility of Course/Faculty Leaders. Learning Resources Development Manager would be expected to check that all relevant content has been made available ahead of the academic year and advise the Vice Principal HE if necessary.

Student Services information

8.12 This information is created and vetted by a dedicated team of staff with the Student Services Manager taking final responsibility for published information. All information is updated on a regular basis with a complete annual update prior to the start of the academic year.

Internal Information for Staff

8.13 This refers to public information communicated to staff on Institution policies, procedures and other guidance mechanisms held on the Institution VLE. Departmental managers have responsibility for ensuring that the information is current and organised appropriately within their own area. Only nominated staff within each department can post or remove information.

8.14 Institution policies are managed centrally by the HE Quality Operations Manager with the published information on our website as part of the information publication scheme. Only the owners of each policy can make amendments and each owner has to pass the updates to the Principalship for approval. All policies are subject to annual review and approval at specified dates. Information we are legally required to published will be monitored by the Head of Governance and such information will be disseminated to the information committee for inclusion in the information publication set online. Responsibility for the updating of the model publication set lies with the Head of Quality Operations.

Monitoring and Evaluation

Review activity

8.15 The information committee will have a standard agenda item for members to report back on any updates which require action from the group such as changes to legal reporting requirements, policy and procedure updates, deadlines for information required for the next academic year.

8.16 Any breaches of procedure will be raised by the Head of Marketing and Recruitment and a decision will be made immediately whether the communications need to be withdrawn and HR advice taken.

Consumer Law

8.17 Students have consumer rights. Universities and other higher education providers that don’t meet their obligations to undergraduate students may be in breach of consumer protection law. This procedure sets out to ensure that The Northern School of Art meets its obligations for consumer law that applies to information provision. Relevant staff within the organisation who have responsibility for external information

are obligated to follow Competitions and Markets Authority guidance, which is why all external relations require approval as set out within this procedure.

Advertising Standards

8.18 We also have obligations to abide by the UK Advertising Code, as regulated by Advertising Standards Authority. Relevant staff within the organisation who have responsibility for external information are obligated to follow ASA guidance, which is why all external relations require approval as set out within this procedure.

EQUALITY AND DIVERSITY IMPACT ASSESSMENT SCREENING

Under the Equality Act, there are nine protected characteristics:		
▪ gender reassignment ▪ marriage and civil partnership ▪ pregnancy and maternity	▪ race ▪ religion or belief ▪ age	▪ sex ▪ sexual orientation ▪ disability

Assessment:

Is this policy/procedure relevant in terms of equality related to the protected characteristics above? Yes ☐ No ☐ If no, please state why not:	
This is general policy relating to all students.	
Is there potential for any negative or positive impact on people with protected characteristics? Yes ☐ No ☐ If yes, Please provide details:	
Positive	Negative
Could this policy or procedure discriminate or unfairly disadvantage people with protected characteristics? Yes ☐ No ☐ If yes, please provide details:	
The Policy has an inclusive approach to students from all backgrounds.	
Conclusion:	
☐ No barriers identified	
☐ Adaptions or changes to the policy or procedure to eliminate bias	
☐ Barriers and impact identified, however, having considered all available options there appear to be no other proportionate ways to achieve the aim of the policy or practice (e.g. in extreme cases or where positive action is taken). Therefore, proceed with caution with this policy or practice knowing that it may favour some people less than others, providing justification for this decision.	

Completed by:

Name:		Job Title:	
Name:		Job Title:	

APPROVAL PROCESS

This document was APPROVED by Principalship on:	XX September 2025
Principalship member with primary responsibility:	Stuart Slorach, Vice Principal (Resources)
Other staff consulted by primary Principalship member:	Martin Raby – Principal
	John Waddington, Vice Principal (HE)
	Mike Wheaton – Vice Principal (Planning & Strategy)
	Rob Kane – Vice Principal (FE)
	Amy Crossland – Vice Principal (People Services)
	Bill Goodwin, IT Manager
	Majahid Irfan Aslam – Systems Development Manager

Elements of this document have been reviewed and approved by School Committees:

Section	Committee	Approval Date