Version number:	Status:	Owner:	Approved By:	Date Approved:	Next Review Date:
2	Draft	Paul Vincent	Will Woods	20 July 2023	1 August 2023

OCA Information Security Policy Set

Updated: July 2023

Workspace Security Policy

Password and Authentication Policy

Acceptable Use Policy

Email and Communications Policy

Cyber Security Policy

Remote Access Policy

Access Control Policy

Information Classification Policy

Information Security Incidents Policy

Information Encryption Policy

Media Disposal Policy

Using Personal Devices for College Business Policy

Third Party Suppliers Management Policy

Payment Card Security Policy

Purpose

The purpose of this policy set is to establish the requirements upon applications, systems, data and individuals in regards to ensuring the Confidentiality, Integrity and Availability of information assets and systems across the college and the contexts in which it operates and provides service.

Values / principles

This policy relates to the following Principles:

Version number:	Status:	Owner:	Approved By:	Date Approved:	Next Review Date:
2	Draft	Paul Vincent	Will Woods	20 July 2023	1 August 2023

- Data Protection and Privacy by Design
- Confidentiality Integrity and Availability (CIA)
- Safeguarding of employees and students

Scope

This policy applies to all college employees and users of its systems and information assets, inclusive of third parties and contractors.

Enforcement

Any breach of these policies is significant as it may undermine the effective running of the OCA and its ability to meet its duties and legal obligations. Failure to comply may lead to disciplinary action in accordance with the college's Disciplinary Policy and Procedure, including dismissal for serious or repeated breaches. It may also be the case that your conduct and/or action(s) may be unlawful. OCA reserves the right to inform the appropriate authorities in such cases. You should note that you may be personally liable for actions and or conduct arising from the use of OCA Systems.

Exception to policy

1.1 Exceptions to these Information Security policies will be considered where there is a justified requirement and the additional risk and/ or cost to mitigate that risk can be balanced with the business benefit.

1.2 For an exception to be considered an IT Security Exception request form must be completed.

1.3 All exception requests will be considered and processed by the IT Services manager and/or the Head of Technology and Innovation.

1.4 Approved exceptions to policy requests will be logged and regularly reviewed.

Changes

This is the first version of the Information Security Policy.

Version number:	Status:	Owner:	Approved By:	Date Approved:	Next Review Date:
2	Draft	Paul Vincent	Will Woods	20 July 2023	1 August 2023

Policies superseded by this document

This policy supersedes the UCA Information Security Policy.

Related policies and legislation

- Data Protection and Confidentiality Policy
- Data Protection Impact Assessment (DPIA) Policy
- Disciplinary Policy and Procedure
- Flexible Working Policy
- Health and Safety Policy
- Wellbeing Policy
- UK Data Protection Act 2018
- UK NIS Regulations 2018
- EU GDPR 2016

Version number:	Status:	Owner:	Approved By:	Date Approved:	Next Review Date:
2	Draft	Paul Vincent	Will Woods	20 July 2023	1 August 2023

Workspace Security Policy

Purpose

The purpose of this policy is to establish best practices for and expectations from employees in regards to their immediate working environments.

Scope

This policy applies to all college employees and users of its systems and information assets.

Changes

This is the first version of the Information Security Policy.

Policies superseded by this document

This policy supersedes the *Workspace Security Policy, November 2021*.

Policy

Appropriate measures must be taken when using workspaces to ensure the confidentiality, integrity and availability of sensitive information, including protected health information (PHI) and that access to sensitive information is restricted to authorised users.

1. College employees using workspaces either provided by the college or established in a remote, e.g. home, environment shall consider the sensitivity of the information, including protected health information (PHI) that may be accessed and minimise the possibility of unauthorised access.
2. OCA will implement physical and technical safeguards for all college-provided workspaces and services that access sensitive information to restrict access to authorised users.
3. Appropriate measures include:

- Restricting physical access to workstations to only authorised personnel.
- Securing devices (screen lock or logout) prior to leaving the area to prevent unauthorised access.
- Enabling a password-protected screen saver with a short timeout period to ensure that devices left unsecured will be protected. The password must comply with the Password and Authentication Policy.

- Complying with all applicable password policies and procedures. See the Password and Authentication Policy.
- Ensuring devices are used for authorised business purposes only.
- Never installing unauthorised software on workstations.
- Storing all sensitive information, including protected health information (PHI) in secured environments, e.g. Filemaker, or approved cloud storage, e.g. Google Drive or MS OneDrive.
- Keeping food and drink at a safe distance from devices in order to avoid accidental spills. Drinks should be kept sufficiently far from electrical devices that they cannot spill ‘on to’ the device, so that a device may be lifted before the fluid makes contact.
- Securing laptops that contain sensitive information by using cable locks or if leaving a device on-site at the end of the day, locking laptops/other devices up in the lockers provided.
- Complying with the Information Encryption Policy
- Installing privacy screens, filters or using other physical barriers to alleviate the risk of exposing data.
- Ensuring workstations are left on but logged off in order to facilitate after-hours updates.
- Exit running applications and close open documents
- Ensuring that all workstations use a surge protector (not just a power strip) or a UPS (battery backup).
- If wireless network access is used, ensure access is secure by following the Wireless Communication policy.

Version number:	Status:	Owner:	Approved By:	Date Approved:	Next Review Date:
2	Draft	Paul Vincent	Will Woods	20 July 2023	1 August 2023

Password and Authentication Policy

Purpose

The purpose of this policy is to establish a standard for creation of strong passwords and the protection of those passwords.

Scope

The scope of this policy includes all staff who have or are responsible for an account (or any form of access that supports or requires a password) on any system that resides at any OCA facility, has access to the OCA network, or stores any non-public OCA information.

Changes

Information previously contained in the superseded Password and Authentication Policy has been reformatted and incorporated into this Information Security Policy Set document.

Additional information incorporated, on 'Application Development and Acquisition' and 'Biometric authentication'.

Policies superseded by this document

This policy supersedes the *Workspace Security Policy, November 2021*.

Policy

1. Password Creation

1.1 All user-level and system-level passwords must conform to the Password Construction Standard.

1.2 Users must use a separate, unique password for each of their work related accounts. Users may not use any work related passwords for their own, personal accounts.

1.3 User accounts that have system-level privileges granted through group memberships or programs such as sudo must have a unique password from all other accounts held by that user to access system-level privileges. In addition, it is required that multi-factor authentication is used for any staff-held accounts.

Version number:	Status:	Owner:	Approved By:	Date Approved:	Next Review Date:
2	Draft	Paul Vincent	Will Woods	20 July 2023	1 August 2023

2. Password Change

2.1 Passwords should be immediately changed when there is reason to believe a password has been or may be compromised.

2.2 Google Workspace account passwords must be changed every 3 months.

2.3 WiFi passwords must be changed whenever an employee leaves the organisation.

3. Password Protection

3.1 Passwords must not be shared with anyone, including supervisors and coworkers. All passwords are to be treated as sensitive, Confidential OCA information.

3.2 Beyond password resets and initial temporary passwords, passwords must not be inserted into email messages, or other forms of non-encrypted electronic communication, nor revealed verbally over the phone to anyone.

3.3 Employees’ passwords may be stored only in “password managers” that have been authorised by the college.

3.4 Do not use the "Remember Password" feature of applications (for example, websites) that have not been endorsed by the college.

3.5 Any user suspecting that their password may have been compromised must report the incident and change their password immediately. Other accounts that may have shared the compromised password should also have their passwords changed.

4. Application Development and Acquisition

Application developers or those responsible for acquiring new applications for use by college stakeholders must ensure that those applications contain the following security precautions:

4.1 Applications must support authentication of individual users.

4.2 Applications must not store passwords in clear text or in any easily reversible form.

4.3 Applications must not transmit passwords in clear text over networks.

4.4 Applications which support Single Sign On (SSO) through secure means (SAML, OAUTH, LDAP) should be prioritised over those which do not provide SSO options.

5. Multi-Factor Authentication

5.1 College staff and contractors with access to sensitive data relating to individuals or systems must use Multi-factor / two-step authentication for their college Email accounts. Multi-factor authentication is highly encouraged for students and should be used whenever possible, not only for work related accounts but personal accounts also.

6. Password Construction Standard

Strong passwords are long, the more characters you have the stronger the password. We recommend a minimum of 10 characters in your password. In addition, we highly encourage the use of passphrases; passwords made up of multiple words, symbols and numbers. Examples include “Some@rtworkLie$!” or “R0undMyW@yMiceB@rk”. Passphrases are both easy to remember and yet meet the strength requirements. Poor, or weak, passwords have the following characteristics:

- Contain eight characters or less.
- Contain no symbols or numbers.
- Contain personal information such as birthdates, addresses, phone numbers, or names of family members, pets, friends, and fantasy characters
- Contain number patterns such as aaabbb, qwerty, zyxwvuts, or 123321
- Are some version of “Welcome123” “Password123” “Changeme123”

In addition, every work account should have a different, unique password. To enable users to maintain multiple passwords, we highly encourage the use of ‘password manager’ software that is authorised and/or provided by the organisation. Whenever possible, also enable the use of multi-factor authentication.

7. Biometric authentication

Using biometric sensors and data in the form of fingerprints and facial recognition in order to access college systems without a password is permitted as long as the precautions outlined in the Password and Authentication Standard are followed.:

- 2-Factor authentication is also enabled on your college account.
- The device being used to authenticate into the college system is encrypted and password and/or pin code protected.
- You agree to notify the college immediately if any device used to access college systems is either lost, stolen or compromised in some way.

Version number:	Status:	Owner:	Approved By:	Date Approved:	Next Review Date:
2	Draft	Paul Vincent	Will Woods	20 July 2023	1 August 2023

Acceptable Use Policy

Purpose

The purpose of this policy is to outline the acceptable use of computer equipment and services at OCA. These rules are in place to protect the employee and OCA. Inappropriate use exposes OCA to risks including virus attacks, compromise of network systems and services, and legal issues.

Scope

This policy applies to all college employees, contractors, consultants, temporaries, and other workers at OCA.

Policy

1. OCA proprietary information stored on electronic and computing devices on site or in the cloud, whether owned or leased by OCA, the employee or a third party, remains the sole property of OCA.
2. You have a responsibility to promptly report the theft, loss or unauthorised disclosure of OCA proprietary information.
3. You may access, use or share OCA proprietary information only to the extent it is authorised and necessary to fulfil your assigned job duties.
4. All mobile and computing devices that connect to the internal network must comply with the Network Security Policy.
5. System level and user level passwords must comply with the Password and Authentication Policy. Providing access to another individual, either deliberately or through failure to secure its access, is prohibited.
6. Access to digital resources must be in accordance with the OCA's mission and values. All users must comply with all applicable laws, regulations, and policies.
7. All digital resources must be used in a professional and ethical manner. All users must respect the privacy, confidentiality, and intellectual property rights of others.
8. Users must not use digital resources for any illegal, unethical, or immoral purpose, including but not limited to hacking, piracy, or copyright infringement.
9. All users must protect digital resources from unauthorised access, theft, and damage. Users must not disclose their passwords to anyone, including colleagues and family members.
10. Users must report any suspicious or unauthorised activity to the OCA's IT department immediately.

Version number:	**Status:**	**Owner:**	**Approved By:**	**Date Approved:**	**Next Review Date:**
2	Draft	Paul Vincent	Will Woods	20 July 2023	1 August 2023

11. All users must comply with the OCA's Data Protection policies, including the General Data Protection Regulation (GDPR) and UK Data Protection Act.
12. Employees must comply with OCA's Email and Communications policies, standards and procedures while working remotely.
13. Employees who work remotely must ensure that their work area is safe and secure, free from distractions and potential security breaches.
14. Employees must comply with the OCA's Information Classification and Encryption policies, standards and procedures when working with sensitive data or information.
15. All users must comply with the OCA's Health and Safety policies and procedures.

Version number:	Status:	Owner:	Approved By:	Date Approved:	Next Review Date:
2	Draft	Paul Vincent	Will Woods	20 July 2023	1 August 2023

Email and Communications Policy

Purpose

This Email and Communications Policy outlines the acceptable use of email and all forms of digital communication by employees of the Open College of the Arts (OCA). This policy covers all communication methods, including email, instant messaging, video conferencing, and phone calls. All employees are expected to adhere to these guidelines to maintain the integrity, security, and professionalism of the OCA's communication systems.

Scope

This policy applies to all college employees, contractors, consultants, temporaries, and other workers at OCA.

Policy

1. All communication must comply with the OCA's mission and values. All employees must adhere to all applicable laws, regulations, and policies.
2. All communication must be professional, courteous, and respectful. Employees must not use inappropriate language, engage in harassment or discrimination, or make discriminatory remarks.
3. All communication must be relevant to the OCA's business. Employees must not use OCA's communication systems for personal or non-work-related purposes.
4. Employees must use their OCA email accounts for all work-related communication. The use of personal email accounts for OCA business is prohibited.
5. Employees must not share their OCA email passwords or any other login credentials with anyone else, including family members or colleagues.
6. Employees must not use email or other communication systems to transmit confidential or sensitive information unless they have been authorised to do so.
7. The use of non-approved third-party communication tools is prohibited without prior approval from the OCA's IT department.

Version number:	**Status:**	**Owner:**	**Approved By:**	**Date Approved:**	**Next Review Date:**
2	Draft	Paul Vincent	Will Woods	20 July 2023	1 August 2023

8. All employees must use appropriate language and tone when communicating with colleagues, clients, and partners. Employees must not engage in any form of harassment or discrimination.

9. All video conferencing and phone calls should be scheduled in advance wherever possible and must be relevant to the OCA's business.

10. Employees must follow the OCA's guidelines for virtual meetings, including muting microphones when not speaking, using appropriate virtual backgrounds, and adhering to the dress code.

Version number:	Status:	Owner:	Approved By:	Date Approved:	Next Review Date:
2	Draft	Paul Vincent	Will Woods	20 July 2023	1 August 2023

Cyber Security Policy

Purpose

The purpose of this policy is to establish the requirements upon applications, systems, data and individuals in regards to ensuring the Confidentiality, Integrity and Availability of information assets and systems across the college and the contexts in which it operates and provides service.

Scope

This policy applies to all college employees and users of its systems and information assets.

Changes

This is the first version of the Cyber Security Policy.

Policies superseded by this document

This policy supersedes the UCA Information Security Policy.

Policy

1. Mitigating Controls in Place

1.1 Protection against Malware

1.1.1 All college-supplied laptops and other computing devices are installed with anti-virus and the drives encrypted.

1.1.2 All Operating Systems are set to apply security updates automatically, with urgent patches not covered by Operating System updates applied centrally by the IT Team either on-site or through the use of remote access connections.

1.1.3 The College Password and Authentication policy establishes minimum password length and additional security requirements as protections against malware.

1.1.4 Mandatory staff training is in place to educate individuals in the risks and current approaches in use regarding phishing attempts which can otherwise lead to the installation of malware.

1.2 Management of the College Network and Connectivity Security

1.2.1 Head Office WiFi is managed by Barnsley Council (BMBC). The password is reset every 3 months. HR systems issue a ‘Leaver Details’ notice to IT Services detailing the employee’s last working day; Wifi and any other shared passwords are centrally reset by IT Services at the end of that working day..

1.3 Management of Endpoint Security

1.3.1 All college-provided computing devices’ drives are encrypted through centrally-administered security policies to reduce the risk of a data breach in the event of theft, loss or intrusion.

1.3.2 Windows-based computing devices are authenticated through and centrally managed by Google Workspace, inclusive of 2-Step Authentication requirements for access and central revocation of access to, or wiping of, the device in the event of theft, loss or intrusion.

1.3.3 Secure storage lockers are provided for staff to secure their computing devices in the college’s office space when not required off-site.

1.4 Management of User Identities and Access

1.4.1 All college staff are issued with a Google Workspace account, which is used to access core services via secure SAML or OAUTH authentication methods.

1.4.2 As per the college’s Passwords and Authentication Policy, all members of college staff must have 2-step Authentication enabled on their Google Workspace account.

1.4.3 The principle of ‘Least Privilege’ is applied to all Information Systems.

1.5 Information Asset Management

1.5.1 The college’s Information Assets are itemised in its Data Mapping document. All new and updated information assets are registered against purpose, location, type, classification and owner.

1.5.2 Information Asset Owners are responsible for the classification and categorisation of their assigned assets.

1.5.3 Information Asset Owners are responsible for ensuring that assets assigned to them are correctly shared and secured in line with the asset's security classification.

1.6 Management of Physical access to IT Equipment

1.6.1 The OCA offices are accessible only to employees in possession of a provided key card. Key cards must not be loaned to any other individual.

1.6.2 Loss of a staff key card must be immediately reported to the IT Team and to the DMC administrative staff at dmc@barnsley.gov.uk.

1.6.3 Each member of Head Office and Programme Leader staff will be issued a college laptop for business use. No other device may be used for college business on the internal OCA network unless authorised by the IT Team in advance.

1.6.4 Any loss of college provided IT equipment must be immediately reported to the IT Team in order for accounts to be secured and potential data breaches to be investigated.

1.6.5 Devices must be locked whilst unattended.

2. Incident Response

2.1 All users of OCA IT systems are required to report breaches of both data and policy, including any identified threats and vulnerabilities to the IT Service Desk.

2.2 All IT systems and associated services must make provision for the alerting of the IT Team to any data breaches and other malicious intrusions.

2.3 An Information Security Incident Response Plan must be maintained and aligned to unit incident plans, tested by the Information Security Team, and circulated to all relevant parties.

2.4 The OCA will maintain the capability to detect and respond to unauthorised access, disclosure, modification, or loss of information on OCA information systems.

2.5 The Incident Response Plan and incidents relating to information systems which process, store and/or transmit payment card information must adhere

Version number:	Status:	Owner:	Approved By:	Date Approved:	Next Review Date:
2	Draft	Paul Vincent	Will Woods	20 July 2023	1 August 2023

to all applicable requirements in the Payment Card Industry Data Security Standard (PCI DSS).

3. Corrective Response

3.1 The college's 'OCA Central' storage space held on its Google Drive service is required to be used by all staff for the storage of Business Critical and (wherever possible) BAU assets. This storage space is frequently backed up to two securely encrypted locations for corrective access in Disaster events or Incidents which involve the destruction of, or removal of access to, essential data e.g. Ransomware attacks.

3.2 Business-critical systems are backed up at least daily in order that they might be reinstated in the event of a Disaster event or Malicious activities impacting access to those systems.

Version number:	Status:	Owner:	Approved By:	Date Approved:	Next Review Date:
2	Draft	Paul Vincent	Will Woods	20 July 2023	1 August 2023

Remote Access Policy

Purpose

This policy establishes the measures which must be adhered to when accessing college systems outside of the college's central network at its head office premises.

Scope

This policy applies to all college employees and users of its systems and information assets.

Changes

This is the first version of the Remote Access Policy.

Policies superseded by this document

This policy supersedes the UCA Information Security Policy.

Policy

1. Responsibilities

1.1 General access to the Internet for recreational use through the OCA network is strictly limited to OCA employees, contractors, vendors and tutors (hereafter referred to as "Authorised Users").

1.2 When accessing the OCA network from a personal computer, Authorised Users are responsible for preventing access to any OCA computer resources or data by non-Authorised Users.

1.3 Performance of illegal activities through the OCA network by any user (Authorised or otherwise) is prohibited. The Authorised User bears responsibility for and consequences of misuse of the Authorised User's access. For further information and definitions, see the Acceptable Use Policy.

Version number:	Status:	Owner:	Approved By:	Date Approved:	Next Review Date:
2	Draft	Paul Vincent	Will Woods	20 July 2023	1 August 2023

2. Requirements

2.1 Secure remote access must be strictly controlled with encryption (i.e., Virtual Private Networks (VPNs)) and strong pass-phrases. For further information see the Password & Authentication Policy.

2.2 Authorised Users shall protect their login and password, even from family members.

2.3 While using an OCA-owned computer to remotely connect to OCA's network, Authorised Users shall ensure the remote host is not connected to any other network at the same time, with the exception of personal networks that are under their complete control or under the complete control of an Authorised User or Third Party.

2.4 Use of external resources to conduct OCA business must be approved in advance by the ICT team and the appropriate dept. manager.

2.5 All hosts that are connected to OCA internal networks via remote access technologies must use the most up-to-date antivirus software, this includes personal computers.

2.6 Personal equipment used to connect to OCA's networks must meet the requirements of OCA-owned equipment for remote working.

2.7 Systems and applications which store sensitive personal data relating to college stakeholders must be sufficiently protected by at least one of the following means:

- IP Address limitation: any employee requiring remote access must inform the ICT Team of their internet-facing IP address and confirm that the network being used to access the system is secure.
- 2-Factor Authentication: access to the system only permitted through use of two or more authentication methods. E.g. SMS or Authenticator application codes, USB Key, or biometric authentication in addition to a secure password.

Support

For additional information regarding OCA's remote access connection options, including how to obtain a remote access login, free antivirus software, troubleshooting, etc., support is available through the college’s IT Services team: ithelpdesk@oca.ac.uk

Version number:	Status:	Owner:	Approved By:	Date Approved:	Next Review Date:
2	Draft	Paul Vincent	Will Woods	20 July 2023	1 August 2023

Access Control Policy

Purpose

This policy outlines the checks, safeguards and principles relating to the control of access to college-controlled data.

Scope

This policy applies to all employees of the college (inclusive of external contractors and other third parties), in addition to the systems it owns and/or uses.

Changes

This version of the Access Control Policy has been completely revised.

Policies superseded by this document

This policy supersedes the college's adoption of the UCA Information Security Policy.

Policy / procedure

1. Users' information and information systems

1.1 By using OCA computers and its associated networks and applications, all users are agreeing to abide by The Open College of the Arts (OCA) Information Security policies. Usage is also subject to the legal requirements of the Computer Misuse Act and the Data Protection Act.

1.2 You may only use computers and computer accounts that you have been officially authorised to use.

1.3 Users must not intentionally disclose their username to anyone outside of the OCA.

1.4 Provisioned usernames grant access to OCA information and information systems and are required for a user's job role and responsibilities. Users must only access information for which they have appropriate authorisation.

1.5 The OCA will actively monitor IT information systems for the detection and prevention of unauthorised access.

1.6 It is the responsibility of every user to report any unauthorised access or suspected compromise of their account to the IT Help Desk (helpdesk.oca.ac.uk) and to ithelpdesk@oca.ac.uk.

1.7 Information systems which process, store and/or transmit payment card information must adhere to all applicable requirements mandated in the Payment Card Industry Information Security Standard (PCI DSS).

2. All approvers and administrators of access control configurations on information systems

2.1 Privileged server administrator accounts must only access OCA information systems when logged on to an OCA managed computer.

2.2 Access to OCA information and information systems must be granted through the provision of a unique username.

2.3 Access Granted to college systems must follow the ‘least privilege’ principle, only granting access required for the user’s job role.

2.4 Access to OCA information and OCA information systems must be granted through an approved documented process and follow best practice guidelines. Each documented process must be reviewed and approved on an annual basis.

2.5 Information Owners and Approvers of access requests to information systems must review and validate user accounts and permissions granted at least annually and an audit trail of validation evidence maintained.

2.6 Administrator or ‘root’ access to OCA information systems will be limited to staff whose job roles require it.

2.7 Staff and Administrator accounts must use Multifactor authentication.

2.8 Administrator or ‘root’ accounts must only be used to facilitate tasks where elevated privileges are required.

2.9 For compliance, auditing and reporting purposes the use of generic IDs that are shared and not assigned to a specific named individual are restricted and should only be provisioned after an exception request is raised and approved.

2.10 Where possible, systems that cannot authenticate directly with Google Workspace should use ADFS to accomplish a single sign-on for all systems.

3. Third party use of OCA information and information systems

3.1 Public facing systems which facilitate access to Highly Confidential information will be subject to an Information Security risk assessment to assess if further controls are required such as two-factor authentication.

3.2 External access to the OCA's Google Workspace environment using Groups, Chat, Meet, Calendar or Drive/Docs may be permitted in cases where the activity relates to data with a classification of Internal Only or Public. External is defined as those without an OCA and/or an OCA email address. Permission for externals must be explicitly approved by the Information Asset Owner.

3.3 Where temporary external access to OCA systems is required and which results in exposure of individuals' personal data, an NDA must be drafted and issued to the external individual or business entity, and returned to the Information Asset Owner prior to any access being granted. The DPIA Policy should also be consulted and its processes followed, in conjunction with the acquisition of a signed NDA.

4. Physical access to networks and devices

4.1. Physical access to college-leased or owned properties must incorporate measures to limit ingress and egress only to identifiable employees and other authorised individuals.

4.2. Employees are responsible for ensuring the physical security of their college-provided equipment, both on- and off-site.

4.3. Only individuals approved by the IT Services Manager or Head of Technology and Innovation may access server equipment, including any backup media securely stored outside of data centres or server rooms.

Version number:	Status:	Owner:	Approved By:	Date Approved:	Next Review Date:
2	Draft	Paul Vincent	Will Woods	20 July 2023	1 August 2023

Information Classification Policy

Purpose

This policy establishes the range of information classification types and provides examples of their application in an OCA context.

Scope

This policy applies to all college employees and users of its systems and information assets.

Changes

This is the first version of the Information Classification Policy.

Policies superseded by this document

This policy supersedes the UCA Information Security Policy.

Policy / procedure

1.1 The Information Asset Owner of any information set created is responsible for assigning the appropriate information classification in accordance with this policy.

1.2 Information asset ownership may be transferred upon agreement with the newly identified Information Asset Owner.

1.3 OCA information in any form must be managed in accordance with Information Security policies, and the Data Protection and Confidentiality Policy.

1.4 Information Asset Owners should understand the administrative and technical controls for which they are accountable and responsible, and an awareness of those operated by IT Services, to safeguard information in accordance with its classification.

1.5 Where information has not received an information security classification, the ‘Highly Confidential’ classification must be assumed and applied.

1.6 To align to UK Government Classification Policy, OCA Proprietary aligns to Official, OCA Highly Confidential aligns to UK Official-Sensitive. OCA Highly Restricted aligns to UK Secret. Security Controls must be agreed before the storage of UK Secret information. The OCA is not equipped to handle UK Top Secret Information.

Classification

Classification	Description	OCA-specific Example
Highly Restricted	Information that requires controls above those implemented by the College to manage Highly Confidential information. Typically these controls are required for information types rarely handled by the College. For example, information where its loss could cause widespread loss of life or else threaten the security or economic wellbeing of the country or friendly nations. Information of this nature would require specific controls that must be supplied by the Information Asset Owner and must be adhered to by users of the information.	No normal line of business information falls into this category. Examples would include sensitive defence or medical research information.
Confidential	Information that, if made public or inappropriately shared around the organisation, could seriously impede the organisation's operations and is considered critical to its on- going operations or the College's legal obligations under data protection regulations. Information may include accounting information, sensitive business plans, sensitive customer information of banks, solicitors, and accountants etc., medical records and similar highly sensitive information. Such information should not be copied or sent to third parties without specific authority. Security at this level should be at the highest	Student personal details Employee Personnel records Some types of research information Sensitive business papers Banking details, payment card details (PCI) Organisational Risk registers containing confidential information Financial records Other items covered under data Protection Legislation. Alumni and Donor information

	level for the College’s normal operational requirements.	
Proprietary	Information of a proprietary nature; procedures, operational work routines, project plans, designs and specifications that define the way in which the organisation operates. Such information is normally for authorised personnel only, for proprietary use. Security at this level is high.	Unit and Programme plans Operational plans Software configuration specifications (unless given by agreement to open-source communities) Analysis of anonymised student information.
Internal Use Only	Information not approved for general circulation outside the organisation where its loss would inconvenience the organisation or management but where disclosure is unlikely to result in financial loss or serious damage to credibility. Examples would include internal memos, minutes of meetings and internal project reports. Security at this level is controlled but normal.	Most meeting and committee minutes Team- and Department-specific documentation. Anonymised student information. Copyright-protected educational and promotional resources
Public Documents	Information in the public domain; annual reports, press statements etc.; which has been approved for public use. Security at this level is minimal.	Marketing information Open Educational Resources Open access research information and publications. College statistics and course information intended for public consumption.

Acknowledged Information Asset Owners

Information asset ownership in the College is recorded by the Technology and Innovation Team and is described in the Information roles and responsibilities document.

Version number:	Status:	Owner:	Approved By:	Date Approved:	Next Review Date:
2	Draft	Paul Vincent	Will Woods	20 July 2023	1 August 2023

Information Security Incidents Policy

Purpose

This policy relates to incidents involving a breach of confidentiality, integrity or availability of information assets belonging to students, employees or the public whilst being stored or processed through college systems.

Scope

This policy applies to all college employees and users of its systems and information assets.

Changes

This is the first version of the Information Security Incident Response Policy.

Policies superseded by this document

This policy supersedes the UCA Information Security Policy.

Policy

1.1 All users of OCA information systems are required to report information and policy breaches, system weaknesses and security incidents, to the IT Help Desk and the IT Services team.

1.2 Network, Services and system components must be configured to alert system administrators of security incidents.

1.3 An Information Security Incident Response Plan must be maintained and aligned to unit incident plans, tested by the IT Services Team, and circulated to all relevant parties.

1.4 OCA will maintain the capability to detect and respond to unauthorised access, disclosure, modification, or loss of information on OCA information systems.

1.5 The Information Security Incident Response Plan and incidents relating to information systems which process, store and/or transmit payment card information must adhere to all applicable requirements in the Payment Card Industry Data Security Standard (PCI DSS).

Version number:	Status:	Owner:	Approved By:	Date Approved:	Next Review Date:
2	Draft	Paul Vincent	Will Woods	20 July 2023	1 August 2023

Version number:	Status:	Owner:	Approved By:	Date Approved:	Next Review Date:
2	Draft	Paul Vincent	Will Woods	20 July 2023	1 August 2023

Information Encryption Policy

Purpose

This policy establishes the college's policy in relation to the encryption of data being stored on, transferred from or otherwise processed by college systems and services.

Scope

This policy applies to all college employees and users of its systems and information assets.

Changes

This is the first version of the Information Security Incident Response Policy.

Policies superseded by this document

This policy supersedes the UCA Information Security Policy.

Policy / procedure

1.1 The OCA will provide appropriate encryption capabilities for use on OCA equipment.

1.2 Where passwords are used to secure encrypted data, users must adhere to the Password Policy.

1.3 Where a password or encryption key needs to be shared to enable another party to access encrypted information, the password or key must be communicated separately and securely by a different method.

1.4 Any data written to portable devices and storage from OCA IT equipment must be encrypted.*

1.5 All server management communications must be encrypted.

1.6 Authentication data must traverse external networks in an encrypted format, or utilise an encrypted connection to prevent its unauthorised use.

1.7 Encrypted connections must follow best practice guidelines and industry standards to ensure that the connection is secure.

Version number:	Status:	Owner:	Approved By:	Date Approved:	Next Review Date:
2	Draft	Paul Vincent	Will Woods	20 July 2023	1 August 2023

1.8 Information systems which process, store and/or transmit payment card information must adhere to all applicable requirements mandated in the Payment Card Industry Data Security Standard (PCI DSS).

1.9 The table below defines the minimum security controls required relative to the classification of information and should be adhered to at all times.

Version number:	Status:	Owner:	Approved By:	Date Approved:	Next Review Date:
2	Draft	Paul Vincent	Will Woods	20 July 2023	1 August 2023

Technical Controls

Controls	Highly Restricted (exceptional level of sensitivity)	Highly Confidential (very high level of sensitivity)	Proprietary (high level of sensitivity)	Internal Use (moderate level of sensitivity)	Public (low level of sensitivity)
Data Transmission	**On OCA Network**: Mandated by the Information Asset Owner **Public Network**: Mandated by the Information Asset Owner	**On OCA Network:** Encryption not required **Public Network:** Encryption required	**On OCA Network:** Encryption not required **Public Network**: Encryption required	**On OCA Network:** Encryption not required **Public Network:** Encryption not required	**On OCA Network**: Encryption not required **Public Network:** Encryption not required

Version number:	Status:	Owner:	Approved By:	Date Approved:	Next Review Date:
2	Draft	Paul Vincent	Will Woods	20 July 2023	1 August 2023

Controls	Highly Restricted (exceptional level of sensitivity)	Highly Confidential (very high level of sensitivity)	Proprietary (high level of sensitivity)	Internal Use (moderate level of sensitivity)	Public (low level of sensitivity)
Data Storage	**On OCA network:** Mandated by the Information Asset Owner **Third party storage:** Mandated by the Information Asset Owner **Portable devices and storage:** Mandated by the Information Asset Owner	**On OCA network:** Encryption not required **Third party storage:** Encryption required **Portable devices and storage:** Permitted with encryption for approved devices only with restrictions	**On OCA network:** Encryption not required **Third party storage:** Encryption required **Portable devices and storage:** Permitted with encryption for approved devices.	**On OCA network:** Encryption not required **Third party storage:** Encryption not required **Portable devices and storage***: Permitted without encryption	**On OCA network:** Encryption not required **Third party storage**: Encryption not required **Portable devices and storage*:** Permitted without encryption

*Note that 1.4 implements a stronger safeguard for some data types than stated in the table above to reduce the risk of incorrectly storing sensitive information.

Version number:	Status:	Owner:	Approved By:	Date Approved:	Next Review Date:
2	Draft	Paul Vincent	Will Woods	20 July 2023	1 August 2023

Media Disposal Policy

Purpose

This policy establishes the college's policy in relation to the disposal of any physical or electronic media.

Scope

This policy applies to all college employees and users of its systems and information assets.

Changes

This is the first version of the Information Security Incident Response Policy.

Policies superseded by this document

This policy supersedes the UCA Information Security Policy.

Policy

1.1 Any optical media or hard copy classified as Proprietary or above must be destroyed using a shredder. Please refer to the Information Classification Policy for further details.

1.2 Where IT electronic media has been identified for disposal, the IT Service Desk must be contacted.

1.3 IT electronic media identified for disposal must be tracked in accordance with the Asset Management Lifecycle.

1.4 Where IT electronic media has been identified for reuse within the OCA then secure sanitisation and re-imaging must be undertaken.

1.5 Where IT electronic media has been identified for reuse outside the OCA or for disposal, then a secure wipe to UK Government Communications Electronics Security Group (CESG) approved standards, must be completed by a CESG-approved third party.

Version number:	Status:	Owner:	Approved By:	Date Approved:	Next Review Date:
2	Draft	Paul Vincent	Will Woods	20 July 2023	1 August 2023

Using Personal Devices for College Business Policy

Purpose

The purpose of this policy is to set out the controls for the use of personal devices to strike an appropriate balance between the risks of personal device usage, and the convenience to staff and benefits to students.

Use of personal devices to access college systems, services, and data can be convenient for staff. The ability to perform certain work-related activities from personal devices is also important in serving the needs of students, as it enables staff to respond to students outside of normal working hours.

However, the use of personal devices does create risk to the College, which must be managed. Risks to sensitive College information, including personal information on students and staff, are increased when the device used for access is not under college management control. There is also a greater risk that devices that are not controlled by the College could introduce malicious code into college systems or enable unauthorised individuals to gain access to sensitive College resources.

Overview

Personal devices, sometimes known as Bring Your Own Device(s) or BYOD, refers to any mobile or fixed computing devices (laptops, desktops, smartphones, tablets etc) that are not issued by the College. However, for the purposes of this policy the OCA's definition of BYOD includes 'Autonomous' devices[1]. This policy sets out the requirements and safeguards to allow staff to use personal devices to access College Systems and Services to conduct College business This policy strikes a balance between maintaining an acceptable level of security without imposing unrealistic preconditions on the choice of devices or how they are configured.

Scope

This policy applies to all members of staff (including Flexible Tutors), data processors, partners, suppliers and contractors and others who have authorised access to internal Open College of the Arts services and data.

The policy does not apply to students using personal devices to access student-facing College resources.

[1] These are OCA owned standalone PCs/Macs with restricted access to systems containing proprietary or highly confidential data. They are only for users with specialised needs and these users are responsible for maintaining the security of the devices

Version number:	Status:	Owner:	Approved By:	Date Approved:	Next Review Date:
2	Draft	Paul Vincent	Will Woods	20 July 2023	1 August 2023

Internal College services shall be taken to mean any digital information or service provided by the College and accessible through college controlled networks or over the Internet but excluding College services and information specifically intended for use by and made available to registered students or the general public.

This policy covers the use of electronic devices that have not been issued by the College to store, access, carry, transmit, receive, or use internal College information or College systems, applications, or services on an occasional or regular basis. Such devices include, but are not limited to, smart phones, tablets, laptops, desktop computers and similar technologies.

Definition of 'Personal' devices

For this policy, personal devices should be interpreted to mean any IT device not issued by the College that is used for College purposes to access college-controlled data on an occasional or regular basis.

This includes devices that are owned by, loaned to, rented, or borrowed by the user. Devices provided by a third-party to the user, for example a company laptop used by a contractor or consultant, are also considered 'personal' and in scope of this policy.

Types of personal IT devices include, but are not limited to, smart phones, tablets, laptops, desktops, and other web-connected devices you use that integrate with college systems.

For the purposes of this policy personal devices also includes 'Autonomous' devices provided by OCA. The user of the device is responsible for device maintenance and security.

Policy

1. General policy

1.1 The College takes the security of its information and its responsibilities to comply with relevant legislation seriously. As the user of a personal device used for college business, you are responsible for ensuring that the use of the device complies with this, and other relevant College policies and you accept the potential consequences for non-compliance.

1.2 To access OCA information, users must ensure they have enabled 2-Step Verification on their college Google account or any other account which is being used to store or process college-controlled data.

1.3 Users of personal devices for college business (accessing and/or processing college-owned data or configuring college services) are responsible for ensuring that the device is suitable for the intended purpose, including in its ability to be configured to meet security requirements. Users must ensure:

- Devices and their firmware must be fully licenced, patched and supported by a supplier that produces regular fixes.
- Software must be fully licensed, patched and supported by a supplier that produces regular fixes.
- Critical or High impact patches must be applied within 14 days.
- Unsupported software must be removed immediately.
- All superfluous or unused software and accounts must be removed.
- Devices must have an anti-malware capability, which complies with the Computer Acceptable Use Policy.
- If available, Devices must have an operational firewall e.g., operating system software firewall.
- If available, a password must be set to secure the firewall; this should be set and a unique 12-digit (minimum) password used.

1.4 To ensure OCA maintains its security and legislative compliance, the use of personal devices to store College information must be minimised, both in quantity and in duration. For regular and / or long-term College work or storage of information, College issued equipment should be used, and storage of documents should take place within college systems such as Google Drive or OCA Learn.

1.5 Personal devices may not be used to store master copies of data – only temporary working copies are permitted.

1.6 Users must follow good practice security policies for the type of device in question in how they configure and use the device, particularly in user authentication and storage encryption. If the personal device is used for non-College purposes as well, care must be taken that the other uses of the device do not increase the risk of compromise to college data. These practises include, but are not limited to:

- All devices should be protected by a password, with a minimum length of at least 12 characters.
- Devices should be configured to enable the lock screen after 15 minutes or less of inactivity.
- The device should be configured to lockout after 10 unsuccessful login attempts in 5 minutes.
- Changing all default passwords on devices which have access to OCA data.
- Changing default passwords on devices such as Wi-Fi routers, used to connect to the internet.

- Disabling “auto-run” / ”auto-play” functionality for removable devices/media and files downloaded from the internet.
- Automatic updates should be enabled where available.
- OCA administrator accounts must only be used for administrative activities. Users must not use an administrative account for day-to-day use, such as Email, Office applications or surfing the web.

1.7 If a personal device that has been used for College business is lost, stolen, or has suffered any form of security breach that may result in unauthorised access to College data, this must immediately be reported to the College as a potential security and data protection incident. The incident notification should include details of how the personal device was protected from unauthorised access to data and a description of any College data that the device may contain.

2. Mobile Phones and Tablets

2.1 Mobile device users are responsible for the security of OCA information and of the device on which OCA information is held.

2.2 Mobile device users must only store OCA information for no longer than is absolutely necessary, not be excessive and be securely deleted.

2.3 Mobile device users must not store or transmit OCA information to a cloud computing service unless it is within an OCA negotiated contract.

2.4 Mobile devices must be secured using biometrics (e.g., face or fingerprint scan) or a passcode, passphrase, PIN number or a pattern lock which meets the requirements set out in the password policy.

2.5 Mobile devices must not be left unattended whilst unlocked and must be set to automatically lock after 15 minutes or less.

2.6 Mobile devices must have an up-to-date and supported operating system.

2.7 Mobile devices must not be ‘Jailbroken’ or ‘rooted’ or have otherwise circumvented the installed operating system security requirements.

2.8 Applications must only be downloaded from an official App Store and be signed by the store’s application key.

2.9 OCA information must only be accessed from pre-approved applications.

2.10 Information which is stored on the mobile device (including any removable storage) and is classed as Proprietary or above, must be protected via encryption.

2.11 Mobile device users must promptly inform the OCA IT Services team and DPO of any unauthorised access to OCA information via a mobile device or if the mobile device is lost or stolen. At the owner of the device’s request a remote wipe of the device will be attempted.

2.12 The OCA cannot see any of your personal data on mobile devices, however the OCA reserves the right to monitor and log data traffic transferred between mobile devices and OCA systems.

2.13 Personally owned mobile devices must not access the OCA Staff wireless network, but can access the guest DMC network.

2.14 Personally owned mobile devices must not retain personal information from OCA information systems.

2.15 Personally owned mobile devices must be returned to the manufacturer’s default settings before they are sent for repair, sold, exchanged or disposed. All OCA information must be securely wiped as part of this process.

2.16 Any mobile devices provided by the college must be sufficiently physically secured e.g. with a secure cable lock or locked in pedestal or cupboard and not left unattended in an insecure environment e.g. overnight in a car or desk.

2.17 Mobile devices must not be configured and used as publicly accessible internet ‘hot spots’ while concurrently connected to the OCA network.

2.18 OCA will use posture checking to ensure that OCA-issued devices and personal devices which request to connect to the internal network meet policy requirements.

2.19 OCA reserves the right to deny or restrict access to any mobile device that does not meet policy requirements. This is to preserve the confidentiality, integrity and availability of the OCA network and its systems.

2.20 OCA is the owner of all OCA information processed on Mobile Devices, irrespective of who owns the Mobile Device.

Version number:	Status:	Owner:	Approved By:	Date Approved:	Next Review Date:
2	Draft	Paul Vincent	Will Woods	20 July 2023	1 August 2023

Version number:	Status:	Owner:	Approved By:	Date Approved:	Next Review Date:
2	Draft	Paul Vincent	Will Woods	20 July 2023	1 August 2023

Third Party Suppliers Management Policy

Purpose

This policy establishes the information security requirements in place for establishing a supplier to the college of services, software or hardware.

Values / principles

This policy relates to the following Principles:

- Data Protection and Privacy by Design
- Confidentiality Integrity and Availability (CIA)
- Safeguarding of employees and students

Scope

This policy applies to all college employees and users of its systems and information assets, in addition to service providers and contractors of the college.

Changes

This is the first version of the Third Party Suppliers Policy.

Policies superseded by this document

This policy supersedes the UCA Information Security Policy.

Policy

1. Engagement

1.1 All third parties working on behalf of the OCA must be assigned a Sponsor.

1.2 Any 3rd party service which includes a technology component (such as a website or application) must be registered with the college's central list of technology.

Version number:	Status:	Owner:	Approved By:	Date Approved:	Next Review Date:
2	Draft	Paul Vincent	Will Woods	20 July 2023	1 August 2023

1.3 Introduction of a 3rd party service which includes a technology component must plan for decommissioning at the end of life, or when the service is no longer required.

1.4 Consultation with the IT Services Team should be carried out as early as possible in order to ensure that appropriate due diligence is undertaken, and to identify if a risk assessment is required to ensure that the College is not exposed to undue risk. Where a risk assessment is required, the Information Security Risk Assessment form should be issued to the proposed vendor.

1.5 When engaging with a third party for the first time, a Non-Disclosure Agreement (NDA) must be signed before any OCA information is disclosed.

All third parties engaged to provide services to the OCA must have a contract in place.

1.6 The contract must include the following:

- Confidentiality clause
- Agreement to follow all OCA Information Security policies
- Right to audit clause
- Requirements to keep any technology supported and patched for the duration of the contract.
- Secure disposal of OCA information upon termination of contract.

1.7 All third parties who process personal data on behalf of the College must have a data processor clause written into the commercial contract. The college's Data Protection Officer should be contacted for further information (dpo@oca.ac.uk). All external transfers of personal data from the College to the supplier and from the supplier to other approved parties must be recorded by the supplier and the Data Protection Officer.

1.8 The sponsor is responsible for ensuring that; the appropriate agreements and contracts are in place; the third-party access rights to information and information systems are provisioned in accordance with the Information Asset Owner's approval and that where software development is outsourced to a third party, requirements of the Secure Software Development Policy are implemented.

Version number:	Status:	Owner:	Approved By:	Date Approved:	Next Review Date:
2	Draft	Paul Vincent	Will Woods	20 July 2023	1 August 2023

1.9 All contracts with third parties for the supply of services to the College will be monitored and reviewed to ensure that information security requirements are being satisfied.

1.10 Third parties must notify the OCA of any security incidents impacting OCA information or information systems within the terms specified in the Service Level agreement (SLA)

2. Third party access connections or interfaces to OCA systems

2.1. All third-party connection requests must have approval from the following; Sponsor, Information Asset Owner,and IT Services before being granted.

2.2. Where third party access is granted, connectivity must be provisioned through approved OCA solutions, restricted to the resources required to carry out the work.

2.2.1. Third parties must agree to adhere to OCA Information Security and Data Protection Policies

2.3. Third party connections must be terminated when no longer required and may be terminated in the event of a security breach.

2.4. The OCA will monitor third party connections for the detection and prevention of unauthorised access.

2.5. A central register of all third-party connections will be maintained by the IT Services team and will be reviewed and updated quarterly or as necessary.

2.6. Third party access to information systems which process, store and/or transmit payment card information must adhere to all applicable requirements mandated in the Payment Card Industry Data Security Standard (PCI DSS).

Version number:	Status:	Owner:	Approved By:	Date Approved:	Next Review Date:
2	Draft	Paul Vincent	Will Woods	20 July 2023	1 August 2023

Version number:	Status:	Owner:	Approved By:	Date Approved:	Next Review Date:
2	Draft	Paul Vincent	Will Woods	20 July 2023	1 August 2023

Payment Card Security Policy

Purpose

This policy establishes the protections and precautions that must be exercised when card data is being processed by employees of the college and its systems.

Values / principles

This policy relates to the following Principles:

- Data Protection and Privacy by Design
- Confidentiality Integrity and Availability (CIA)
- Safeguarding of employees and students

Scope

This policy applies to all college employees and users of its systems and information assets.

Changes

This is the first version of the Payment Card Security Policy.

Policies superseded by this document

This policy supersedes the UCA Information Security Policy.

Policy

1.1 The storage of cardholder data as defined by the Payment Card Industry Data Security Standard (PCI DSS) is strictly prohibited.

1.2 Information systems which process and/or transmit payment card information must adhere to all applicable requirements mandated in the PCI DSS.

1.3 It is the responsibility of all project managers and sponsors to ensure that projects are compliant with the PCI DSS Standard where applicable.

1.4 Wherever possible, systems should restrict interfacing directly with the cardholder data environment (CDE) to limit the necessary scope of PCI DSS compliance.

Version number:	Status:	Owner:	Approved By:	Date Approved:	Next Review Date:
2	Draft	Paul Vincent	Will Woods	20 July 2023	1 August 2023

1.5 Card payments may only be accepted using methods approved by OCA Finance Team.

1.6 Each person who has access to payment card data is responsible for protecting the information.

1.7 Any suspected or actual information security breach resulting in the compromise of payment card data must be reported immediately to IT Services team.

1.8 The payment card Primary Account Number (PAN), which is typically 16 digits in length, must never be sent and/or received via email or instant messaging and should be automatically detected and blocked wherever possible.

1.9 A list of all authorised devices and personnel with access to the PCI DSS in scope resources must be maintained by IT Services and the Finance team.

1.10 Non-console, remote administrative access into the card data environment (CDE), must use encryption and multi-factor authentication.

Version number:	Status:	Owner:	Approved By:	Date Approved:	Next Review Date:
2	Draft	Paul Vincent	Will Woods	20 July 2023	1 August 2023

Appendix 1: Glossary of Terms

Term	Definition
ADFS (Active Directory Federation Services)	AD (Active Directory) FS (Federation Service) is a means of establishing Single Sign On (see SSO) and data sharing between two organisations, networks or services by establishing trust.
APs (Access Points) / WAPs (Wireless Access Points)	An AP or WAP is a device with a wired connection to a Router (see Router), or which may be an integral component of the Router itself, that provides wireless access to the internet and/or an internal network for nearby devices.
BAU (Business As Usual)	BAU refers to activities that relate to normal operational activities, rather than isolated or temporary projects.
Domain / Domain Name	A Domain Name is a set of readable words or string of characters that is used to represent a network or portion of a network. E.g. the first part of a website or email address, e.g. oca.ac.uk or bbc.co.uk.
DMZ (Demilitarised Zone)	DMZ is a networking term for a portion of a network that has been separated / isolated from the rest of the network for security reasons. Usually used for processing highly sensitive data, such as Payment Card data (see PCI / DSS)
DPIA (Data Protection Impact Assessment / Data Privacy Impact Assessment)	An assessment that is to be conducted whenever Controlled Data is to be processed in a new or unusual way. A regulatory requirement of all Data Controlling organisations through the UK Data Protection Act 2018 and GDPR (2016.)
DPO (Data Protection Officer)	A DPO assists in the monitoring of internal compliance, informs and advises on data protection obligations, provides advice regarding Data Protection Impact Assessments (see DPIA.)
Encryption	The process of converting plain, readable text and numbers into seemingly random strings of characters.
Encryption at Rest	The process of ensuring that data is secured through

	Encryption techniques (see Encryption) whilst stored.
Encryption In-Transit	The process of ensuring data is encrypted through Encryption techniques (see Encryption) whilst being transmitted/transferred between networked devices.
GDPR (General Data Protection Regulation)	The regulatory framework upon which the UK Data Protection Act 2018 is based, and which all Data Controllers and Data Processors are required to follow when processing the data of EU and/or UK subjects.
ICO (Information Commissioner's Office)	The UK's regulatory body which is responsible for ensuring the compliance
MFA (Multi-Factor Authentication)	A means of enhancing the security of user accounts beyond usernames and passwords (something you know), by requiring the account owner to input a code from an additional device such as a mobile phone or security key fob (something you own.) See also 2FA (Two-Factor Authentication or Two-Step Authentication)
Network	Two or more interconnected computing devices that can communicate and exchange information with one-another.
OAUTH (Open Authorisation)	A secure method of Single Sign On (SSO) authentication, which removes the need for multiple usernames and passwords, and permits the exchange of information between third-party services.
Password Manager	An application or service that simplifies the management of multiple complex passwords by storing them in an encrypted form, ready to be used in login forms.
PCI/DSS (Payment Card Industry Data Security Standard)	(PCI DSS) is a set of security standards formed in 2004 by Visa, MasterCard, Discover Financial Services, JCB International and American Express.
Router	A networking device for sending and receiving data (packets of data) between computing devices, either locally or over the internet. See also APs (Access Points) / WAPs (Wireless Access Points).

SAML (Secure Authenticated Markup Language)	A secure method of Single Sign On (SSO) authentication, which removes the need for multiple usernames and passwords.
SSL (Secure Socket Layers)	A means of establishing a secure, authenticated and encrypted connection between two networked devices.
SSO (Single Sign On)	A means of accessing a networked computing device using the Command Line Interface (CLI).
2FA (Two Factor Authentication, or Two-Step Authentication)	A means of enhancing the security of user accounts beyond usernames and passwords (something you know), by requiring the account owner to input a code from an additional device such as a mobile phone or security key fob (something you own.) See also MFA (Multi-factor Authentication)
VPN (Virtual Private Network)	VPNs are used to protect your privacy whilst using online services, by encrypting your internet traffic and masking your identity and/or location. They are also frequently used to bypass national and corporate firewalls to allow access to otherwise prohibited services.
Wi-Fi (also, WiFi or Wifi)	A wireless communications technology that allows computing devices to connect to the internet through Access Points (see APs.)