Version:4

Date of Issue: 16/07/2024

Trinity College Dublin
Coláiste na Tríonóide, Baile Átha Cliath
The University of Dublin

IT and Cyber Security Policy

Incorporating Supporting Policies

Table of Contents

1. Context

Effective Information and cyber security is essential to the success of all of Trinity College Dublin's core Education and Research activities and the University's operations. This can only be achieved by ensuring all University staff, students and third parties act in accordance with defined policies and operational procedures aligned with international best practices.

The IT and Cyber Security Policy provides a framework in which security threats to University Information Systems can be identified and managed on a risk basis and establishes terms of reference, which are to ensure uniform implementation of cyber security controls throughout the University.

2. Purpose

The Information technology and cyber security policy and supporting policies define the Universities guidelines and provisions for ensuring the security of university data and associated information technology assets.

The policy aims to provide clear guidance to all staff, students, and relevant third parties in the use of the University technology infrastructure and the management of university data.

In addition, the University must meet its compliance obligations and ensure that it operates in line with all relevant national and EU legislation and with government guidelines for the sector.

3. Benefits

Compliance with the information Technology and Cyber Security policy protects University data and technology assets from threats including cyber-attacks, hacking, social engineering, and human error.
The policy facilitates this by providing consistent best practice guidance in all relevant cyber security domains.

4. Scope

The IT and Cyber Security Policy applies to all staff and students of Trinity and to all third parties authorised by Trinity to access University data or any component of the University's technology infrastructure.

5. Principles

The underlying principles of the IT and Cyber Security Policy are to:

- Ensure that information is created, used, and maintained in a secure environment.
- Ensure that all of Trinity's computing facilities, programs, data, network, and equipment are adequately protected against loss, misuse, or abuse.

- Ensure that all Users of Information Technology (IT) at Trinity College Dublin are aware of and fully comply with the IT and Cyber Security Policy Statement and the relevant supporting policies and procedures.
- Ensure that Trinity's teaching, research, administrative and commercial activities do not experience disruption due to preventable cyber security incidents.
- Ensure that all Users are aware of and fully comply with the relevant Irish and European Community legislation.
- Create awareness that appropriate security measures must be implemented as part of the effective operation and support of Information Security.
- Ensure that all Users understand their own responsibilities for protecting the confidentiality and integrity of the data they handle.
- Ensure all College owned Technological Information Systems have an identified owner /administrator.

6. Definitions

Network Users / Users : Network Users are defined as any staff, students, of Trinity College Dublin, subsidiaries, related companies, institutions and research entities, partners, suppliers and other third parties utilising either a Trinity owned, personally owned, or provided computer or other device used to connect directly or remotely to the Trinity network or has been provided with a username and password or other type of authentication that allows access to the network or systems.

Autonomous Managed Networks (AMN's): The autonomously managed networks (AMN's) are separate logical and physical networks created to address specific and specialised needs of a localised user population. They are operated in agreement with IT Services and managed by dedicated full time and suitably qualified staff.

Autonomous Network Manager (Network Manager): Each AMN as defined above appoints a named individual as the AMN manager. That person is responsible for authorising requests locally and liaising with IT Services.

Third Party Access: Third party Access is defined as all local or remote access to the Trinity Network or devices attached to the Trinity Network for any purpose.

Trinity staff: Defined as all current registered employees (full time, part time, including contract, and occasional) of Trinity College Dublin.

Students: Defined as all currently registered students at Trinity College Dublin.

Third Parties: Defined as any individual, group, contractor, vendor or agent not registered as a current Trinity staff member or student who has been granted access to the Trinity network or to Trinity systems or Trinity data. This includes visitors, retired and former staff members, students or Alumni with an active username /password or email account.

Software: Software in this policy is defined as any operating system, application, database, web service, public or private cloud service, AI solution or other IT solution or system that is used to create, collect, process and/or store data in an electronic format.

Trinity Information / Trinity Data: Defined as any data in an electronic format pertaining to Trinity staff, students, or activities of the University, including academic, research and administrative activities. Additionally, any data in an electronic format collected by Trinity or other bodies on behalf of the University.

Information: means Trinity Information / Trinity Data

Data: means Trinity Information / Trinity Data

Technological Information Systems / Information Systems: includes all physical, virtual and cloud Infrastructure, networks, hardware, and software, which are used to create, manipulate, process, transport and/or store Trinity Information or Data.

Systems / IT Systems / University Information Systems: means Technological Information Systems / Information Systems

Personal Information: Defined as data pertaining to any living individual which is subject to the General Data Protection Regulation (GDPR).

Sensitive data: Is defined as financial data, sensitive teaching or research data or personal data.

7. IT and Cyber Security Policy Statement

7.1 Information is a critical asset of Trinity College Dublin hereafter referred to as 'Trinity'. Accurate, timely, relevant, and properly protected information is essential to the success of Trinity's academic and administrative activities. Trinity is committed to ensuring all accesses to, uses of, and processing of Trinity information is performed in a secure manner.

7.2 Trinity College Dublin is committed to maintaining a security model aligned to ISO27001 international standards.

7.3 Technological Information Systems play a critical role in enabling and supporting the day-to-day activities of the University The object of this Cyber Security Policy and its supporting policies is to define the security controls and compliance necessary to safeguard Trinity Information Systems and ensure the security, confidentiality and integrity of the information held therein.

7.4 The Policy provides a framework in which security threats to University Information Systems can be identified and managed on a risk basis and establishes terms of reference, which are to ensure uniform implementation of cyber security controls throughout Trinity.

7.5 Trinity recognises that failure to implement adequate IT and cyber security controls could potentially lead to:

- Financial loss
- Irretrievable loss of Important Trinity Data
- Damage to the reputation of the University
- Adverse Legal and regulatory consequences
- Significant and prolonged disruption to the academic and administrative operations of the University due to cyber attack

Therefore, measures must be in place, which will minimise the risk to Trinity from unauthorised access to, modification, destruction or disclosure of systems and data, whether accidental or deliberate. This can only be achieved if all Users observe the highest standards of ethical, personal and professional conduct. Effective security is achieved by working with a proper discipline, in compliance with legislation and College policies, and by adherence to the codes of practice defined in the supporting policies and Guidance notes (Section 13 of this Policy)

7.6 The IT and Cyber Security Policy and supporting policies apply to all Trinity staff and students, Third Parties and all other Users authorised by Trinity.

7.7 It is a condition of employment that Trinity Staff will abide by the IT and Cyber Security Policy regulations and all related policies made and updated by Trinity from time to time. The policies are an integral part of the Regulations for Students.

7.8 The IT and Cyber Security Policy and supporting policies relate to use of:

- All Networks connected to the Trinity Campus backbone infrastructure.
- All Trinity-owned/leased/rented and on-loan locations and facilities.
- To all private systems, owned/leased/rented/on-loan, when connected to the Trinity network directly, or indirectly.
- To all private systems, owned/leased/rented/on-loan, used by university staff and Students to process Trinity data whether on campus or remotely.
- To all Trinity-owned/licensed data/software solutions, on Trinity and on private systems.
- To all data/programs, networks and systems provided to the University by sponsors or external agencies.
- To all owned/leased/purchased private or public cloud-based systems used by Trinity Users or used to process Trinity data.

7.9 The objectives of the IT and Cyber Security Policy and supporting policies are to:

- Ensure that information is created used and maintained in a secure environment.
- Ensure that all of Trinity's computing facilities, programs, data, network, and equipment are adequately protected against loss, misuse, or abuse.
- Ensure that all Users are aware of and fully comply with the Policy Statement and the relevant supporting policies and procedures.
- Ensure that Trinity's teaching, research, administrative and commercial activities do not experience disruption due to cyber security incidents.
- Ensure that all Users are aware of and fully comply with the relevant Irish and European Community legislation.
- Create awareness that appropriate security measures must be implemented as part of the effective operation and support of Information and Cyber Security.
- Ensure that all Users understand their own responsibilities for protecting the confidentiality and integrity of the data they handle.
- Ensure all College owned assets have an identified owner /administrator.

7.10 The Trinity Board has approved the IT and Cyber Security Policy and supporting policies (www.tcd.ie/about/policies/it-policies/). Under the University Collegiate Governance model, the Board delegates accountability for the implementation of and compliance with the IT and Cyber Security Policy, to the heads of academic and administrative units.

7.11 The Director of IT Services is the IT and Cyber Security Policy owner. The Director of IT Services, the university's Cyber Security Manager and their delegated agents are authorised to take or direct any actions and decisions necessary to enforce compliance with the IT and Cyber Security Policy and associated supporting policies, and/or to protect the University's Technological Information Systems and/or Trinity Data.

8. IT and Cyber Security Governance

Governance Outline

Security of Trinity's IT and data assets cannot be achieved without a coherent governance model that ensures that all IT systems and services in College are operated in accordance with approved policy and best practice.

The Trinity Governance model seeks to clearly define who is authorised to operate University IT systems and services and how individuals and groups wishing to procure or operate new systems or services are approved, governed and are accountable for their cyber security and policy compliance.

8.1.1 Trinity College Data Network

The Trinity College Data Network is the main Trinity network serving the entire staff and student population. This network is managed and operated by IT Services and provides central services and support to all Users.

The services of this main Trinity network are available to all Users including Users who are also members of other Autonomously Managed Networks.

8.1.2 Autonomously Managed Networks

The autonomously managed networks (AMN's) operated under formal agreement with IT Services and must be managed, operated, and secured by dedicated full time and suitably qualified staff. Each AMN appoints a named individual as the AMN Manager. This person is responsible for authorising requests locally, for liaising with IT Services, and is accountable for monitoring and enforcing compliance with the IT and Cyber Security Policy and associated policies.

8.1.3 Authorised Area IT Support Representatives

Authorised Area IT Support Representatives are individuals employed by their academic or administrative area to spend a proportion of their time dealing with and being responsible for IT matters. These individuals may support specific applications and associated equipment and are responsible for their cyber security.

8.1.4 Services to the Trinity Community

Only IT Services and the defined and approved autonomous networks may operate central key central services including but not limited to Email, Internet Proxy, DNS, DHCP, Firewall, General Purpose Servers, Web Servers, Domain Services.

IT Support Representatives may operate specific applications and supporting servers which they must register with IT Services and / or their appropriate AMN managers.

End users or individuals - who are not governed by AMN's or as Area IT Support Representatives - who wish to run complex IT systems such as servers or purchase cloud solutions to process Trinity data must first seek approval from IT Services.

8.1.5 The Network Perimeter

IT Services acts as the only authorised point of contact between the University and the National Research and Education Network - HEAnet.

Access through the network perimeter firewall is managed and operated by IT Services. Individuals located in the main Trinity network must make direct application and receive approval for any access through the firewall via a process defined by IT Services.

Individuals located in other AMN's must make application first to the authorised Autonomous Network Manager of their AMN who will approve the request and pass it on to IT Services.

8.1.6 Communications

Good quality and frequent communications between all parties defined in this model are vital: Communications between Autonomous Networks and Area IT Support Representatives is facilitated by a mailing list and periodic meetings hosted by IT Services.

9. Roles and Responsibility

9.1.1 The Trinity Board

The Trinity Board is responsible for approving the IT and Cyber Security Policy, and for supporting the Director of IT Services in the enforcement of the policies where necessary.

9.1.2 Critical Infrastructure Committee (CIC)

Is responsible for review and approval of significant changes to the policy.

9.1.3 Heads of Academic and Administrative Areas

Heads of academic and administrative areas are required to familiarise themselves with the policies and are accountable for compliance with the Policy in their area. Where a policy breach is identified or reported, Heads of academic and administrative areas must co-operate in ensuring that appropriate action is taken. Heads of academic and administrative areas are obliged to ensure that all IT systems under their remit are formally administered either by an appointed administrator or by IT Services. The cyber security and compliance duties of the administrator are set out in the associated supporting policies.

9.1.4 Autonomous Networks

Where an area operates an autonomous network with a connection to Trinity Backbone, then the respective Autonomous Network Manager is required to ensure that their operations comply with the IT and Cyber Security Policy.

9.1.5 The University's Cyber Security Manager

The University's Cyber Security Manager is responsible for:

- Advising the Board, the College Officers, administrators, and other appropriate persons on compliance with this policy and its associated supporting policies and procedures.
- Reviewing and updating the Cyber Security policy and supporting policies and procedures.
- The promotion of the policy throughout the University.
- Periodical assessments of cyber security controls as outlined in the IT and Cyber Security Policy and supporting policies and procedures.
- Investigating Cyber Security Incidents as they arise.
- Maintaining Records of Cyber Security Incidents. These records will be encrypted and stored securely for six months after which time information pertaining to individuals will be removed. The records will then be held in this anonymous format for a further two years for statistical purposes.
- Reporting to the Board, the University Officers, Committees, administrators, and other appropriate persons on the status of security controls within the University.

9.1.6 Director, IT Services

The Director of IT Services or their deputy is responsible for the management of the Trinity Network and associated services and for the provision of support and advice to all nominated individuals with responsibility for discharging these policies.

9.1.7 Information Systems Users

It is the responsibility of each individual Information Systems user to ensure their understanding of and compliance with this Policy and the associated codes of practice.

All individuals are responsible for the security of University Information Systems and technology assets assigned to them. This includes but is not limited to infrastructure, networks, hardware and software. Users must ensure that any access to these assets, which they grant to others, is for university approved use only, is limited to what is necessary and is maintained in an appropriate manner.

9.1.8 Purchasing, Commissioning, Developing an Information System

All individuals who purchase, commission or develop an Information System or software solution including vendor supplied or cloud hosted solutions for Trinity are obliged to ensure that this system conforms to necessary security standards as defined in this IT and Cyber Security Policy and supporting policies.

Individuals intending to collect, store or distribute data via an Information System must ensure that they conform to Trinity defined policies and all relevant legislation.

9.1.9 Third Parties

Before any third-party users are permitted access to Trinity Information Systems, a written Third-party agreement is required.

Prior to being allowed to work with Trinity Information Systems, satisfactory references from reliable sources should be obtained and verified for all third parties which includes but is not limited to; administrative staff, software support companies, engineers, cleaners, contract and temporary appointments. Data processing, service and maintenance contracts should contain an indemnity clause that offers cover in case of fraud or damage. Independent third-party review of the adequacy of and compliance with information system controls must be periodically obtained.

9.1.10 Reporting of Security Incidents

All suspected data privacy and cyber security incidents must be reported as quickly as possible through an appropriate channel. All University staff and students have a duty to report information security violations and problems to the University's Cyber Security Manager on a timely basis so that prompt remedial action may be taken.

The University's Cyber Security Manager will be responsible for setting up an Incident Management Team to deal with all incidents. Records describing all reported information security problems and violations will be created. These records will be encrypted and stored securely for six months after which time all information pertaining to individuals will be removed. The records will be held in this anonymous format for a further two years for statistical purposes.

9.1.11 Security Controls

All Trinity Information Systems are subject to the information security standards as outlined in this and related policy documents. No exceptions are permitted unless it can be demonstrated that the costs of using the information security standard exceed the benefits, and it is recorded that the cyber risk can be fully mitigated or has been risk accepted.

9.1.12 Compliance with Legislation

Trinity has an obligation to abide by all Irish legislation and relevant legislation of the European Community. The relevant acts, which apply in Irish law to Information Systems Security, include but are not limited to:

- Regulation on Artificial Intelligence (AI Act)
- The General Data Protection Regulation (EU) 2016/679 (GDPR)
- Data Protection Act 2018
- The eprivacy regulations 2011 S.I. No.336 of 2011
- Data Protection Act 2018 (Section 36(2)) (Health Research Regulations)
- Criminal Damages Act (1991) revised 2019
- Child Trafficking and Pornography (Amendment) Act 2004
- Intellectual Property Miscellaneous Provisions Act (2014)
- Copyright and Related Rights Act (2000)
- S.I. No. 59/2012 - European Union (Copyright and Related Rights) Regulations 2012.
- Safety, Health and Welfare at Work Act 2005 (as amended) Non-Fatal Offences Against the Person Act (Revised 2023)
- Electronic Commerce Act (2000)
- ECommerce Directive (2000/31/EC)
- Regulations entitled European Communities (Directive 2000/31/EC) Regulations 2003 (S.I. No. 68 of 2003)
- Criminal Justice Act 2011

- Criminal Justice (Offences relating to Information Systems) Act 2017
- Freedom Of Information Act 2014

The requirement for compliance devolves to all Users, who may be held responsible for any breach of the legislation. Full texts of the most relevant legislation are available from the College Library, IT Services and associated website and the University's Cyber Security Manager.

10. Breaches of Security

10.1.1 Monitoring

IT Services will monitor network activity, reports from the National Cyber Security Centre, other applicable security agencies, and reports from third party contracted security operation centres and take action/make recommendations consistent with maintaining the security of Trinity information systems.

10.1.2 Incident Reporting

Any individual suspecting that there has been, or is likely to be, a breach of information systems / cyber security should contact the University's Cyber Security Manager or the Director of IT Services immediately who will advise Trinity on what action should be taken.

10.1.3 Enforcement

The Director of IT Services or their delegated agent has the authority to invoke the appropriate University disciplinary procedures in response to breaches of the IT and Cyber Security policy, associated policies, processes and controls.

In the event of a suspected or actual breach of security, the Director of IT Services, their delegated agent or the University's Cyber Security Manager may, after consultation with the relevant Administrator where possible but not a required pre-requisite, make inaccessible/remove any unsafe user accounts, data, machines, infrastructure, network, systems, devices or software from the network, or may fully remove external internet access to / from the University.

10.1.4 Legal Implications

Any breach of security of an Information System could lead to loss of security of personal information. This would be an infringement of the General Data Protection Regulation (GDPR) and could lead to civil or criminal proceedings and/or regulator fines. All staff and students are advised to familiarise themselves with and comply with this policy and with the Trinity Data Protection Policy.

10.1.5 Disciplinary Procedures

Failure of an individual student or member of staff to comply with this policy may lead to the instigation of the relevant university disciplinary procedure and, in certain circumstances, legal action may be taken.
Failure of a contractor or third party to comply could lead to the cancellation of a contract and/or legal action.

11. Policy Awareness and Distribution

11.1.1 New Staff and Students

This Policy Statement will be available from IT Services on request. It will also be published on the IT Services web site and accessible from the University Policy Hub. New staff and students will be notified of the relevant policy documents on commencement of employment or student registration.

11.1.2 Existing Staff

Existing staff and students of Trinity, authorised third parties, and contractors given access to the University network will be advised of the existence of this policy statement. They will also be advised of the availability of the associated policies and procedures which are published on the IT Services website.

11.1.3 Logon Banner

Users logging onto the Trinity network will be reminded of their obligations regarding compliance with the IT and Cyber Security Policy via a Logon banner.

11.1.4 Updates

Updates to Policies, procedures, and security controls will be made periodically and updates will be posted to the University Policy webpages and the IT Services website.

11.1.5 Training

Training will be available from IT Services. IT Services will provide training in a variety of formats. All Trinity staff and students must complete any mandated cyber security training in a timely manner. Further information can be accessed on the IT Services website.

12. Risk Assessment and Compliance

12.1.1 Risk Assessment

Risk assessments must be carried out periodically on all technology solutions, this involves reviewing the business value of the information Users are handling and the information systems security controls currently in place. This is to take into account changes to technology solutions, business requirements, data classifications and University priorities, as well as relevant legislation and to allow for the revision of security controls accordingly.

12.1.2 Heads of Academic and Administrative areas

Heads of academic and administrative areas must establish effective risk reduction / risk mitigation / contingency plans appropriate to the outcome of any risk assessment.

12.1.3 University's Cyber Security Manager

The University's Cyber Security Manager will carry out risk assessments, review all risk assessments completed by other parties and highlight any measures needed to reduce risk in Information Security areas.

12.1.4 Internal Audit

The Internal Auditor will facilitate the assessment of compliance with the IT and Cyber Security Policy periodically.

12.1.5 Third Party Audit

Third Party Audits will be carried out at intervals, as deemed necessary by the Internal Auditor an/or the Director of IT Services.

13. Supporting Policies and Guidance Notes

Supporting Policies to the IT and Cyber Security Policy Statement and outlining codes of practice associated with these policies are in the following sections of this document.

Staff, students and any third parties authorised to access the Trinity Network to use the systems and facilities as identified in paragraph 7.9 of this policy, are required to familiarise themselves with the policies and to work in accordance with them.

13.1 Network Security Policy

The Trinity IT network consists of an interconnection of -networked devices. These include computers, printers, scientific devices, Internet of Things (IOT) devices, audio visual equipment, commercial systems, payment devices, network cables and other networking equipment.

Trinity depends heavily upon its IT network for research, teaching and administrative activities. It is essential that the stability, integrity, and security of the Trinity IT network be safeguarded.

This policy defines the Trinity regulations regarding access to the Trinity Network. All Network Users must comply with the following policy statements:

13.1.1 Network Administration Roles and Responsibilities

- IT Services are responsible for the administration of the Trinity backbone network and primary software domains.
- The administration of the Trinity network including network connections, services, addressing and design is the responsibility of IT Services and delegated agents.
- Additional authorised autonomous managed networks exist which are connected to the Trinity Backbone at an authorised connection point.
- Multiple authorised software domains exist within the Trinity network. The administration of these domains including user accounts and other access controls is the responsibility of the appointed administrator.

13.1.2 Connection to the Trinity Network

- Approval for Connection to and use of Trinity network facilities is dependent on compliance with all published IT Services and Trinity Policies.
- All equipment connected to the Trinity network must conform to the appropriate standards as set periodically by IT Services and Autonomous Network Managers and run only across the backbone using protocols supported by Trinity.
- Only IT Services or authorised Autonomous Network Managers may connect devices to the Trinity Network.
- Side-entry connections to the Trinity network, for example via modem connection to the asynchronous port of a workstation, or via wireless devices are permitted only with the approval of IT Services, or the relevant Autonomous Network Manager.

13.1.3 Wireless Networking

The Director of IT Services or their designee is responsible for providing a secure and reliable campus network to support the mission of the University. Under this broad responsibility, the following campus-wide wireless policies apply:

- Only hardware and software consistent with wireless standards approved by the IT Services shall be used for wireless access points.
- All wireless access points shall be registered with IT Services. In the event that a wireless device interferes with other equipment, the Director of IT Services or designee shall resolve the interference as determined by use priority.
- Deployment and management of wireless access points in common areas of the campus is the responsibility of IT Services.

13.1.4 Server Connectivity

The connection and use of a computer running Server operating system software or otherwise functioning as a server must be authorised by IT Services or an appropriate Autonomous Network Manager.

All Servers must have a defined administrator who is responsible for:

- Server administration, maintenance, and monitoring
- Server security including but not limited to data backup, access control, operating system and application updates and security updates.

Trinity reserves the right to bar access to Information Servers containing material considered illegal or likely to bring the Trinity into disrepute. The University also reserves the right to take disciplinary action in these circumstances.

Trinity will not be liable for any loss or damage suffered by the Information Owner as a result of barring access to or removal of material. Where the Information Owner considers that the University has acted disproportionately or inappropriately in barring access to and/or removing the material then they have the right of appeal through the normal Trinity grievance procedures.

In the event that a server is causing an unacceptable level of interference with or risk to the operation of the Trinity network out of normal hours and the owner/administrator cannot be contacted IT Services or the Autonomous Network Manager may take action to disconnect the Server from the network.

13.1.5 Network Access Controls

Access to Trinity network and facilities is restricted to fully authorised Trinity Users. Users are required to access IT facilities using a secure authentication method. Multifactor authentication is preferred and must be used where available.

Additional authentication mechanisms may be required if IT Services, or Autonomous Network Managers deem it necessary.

IT Services and Autonomous Network Managers must ensure that only authorised Trinity Users have access to the network from their systems.

13.1.6 Connection of Privately Owned Equipment (BYOD)

Students may connect properly maintained computing equipment to the Trinity network only with the permission of IT Services. Such systems are subject to all the statutory and the applicable Trinity rules/regulations/policies in force. Properly maintained means that the equipment is regularly updated with latest software security updates and has up to date anti-malware protection in place.

Students may connect private equipment using the relevant service/procedure in the manner outlined by IT Services on the official website.

Other users (staff, third parties) may only connect properly maintained private equipment to the network in circumstances approved by IT Services and by following the current procedures outlined by IT Services on the IT Services website. All private equipment must meet minimum hardware/software requirements and pass appropriate security checks as defined and updated by IT Services in relevant operational procedures.

13.1.7 Network Administration

All network addresses; including IP addresses, must be allocated and administered by IT Services or authorised Autonomous Network Managers.

IT Services must be informed and consulted in advance of any proposed physical re-organisation of the network. This includes requests for extra cabling or the insertion of wireless networking devices within an academic or administrative area. All requests for physical connections to the Trinity backbone must be directed to IT Services.

IT Services, and Autonomous network managers may, on behalf of Trinity, and subject to appropriate consultations, restrict excessive use of the backbone bandwidth.

In the event of unacceptable network events occurring on the network, IT Services, and Autonomous network managers have the right to gain access to and inspect the configuration of devices or equipment on that network and to direct or invoke the immediate removal of any devices or equipment that it believes could be the source of the problem.

In the event of unacceptable events on a network causing problems on another part of the Trinity network or on an external network, IT Services has the right to disable any part of the network as necessary, to remove the source of the problem. While every effort will be made to contact the system owner, Head of academic or administrative area and/or other appropriate persons, this may not always be possible.

13.1.8 Use of Network Facilities

Use of the Network facilities including but not limited to the network, computers, tablets, phones, printers and the facilities associated with the network e.g. software solutions, data, email, Internet, is subject to Trinity's Code of Conduct.

All data/software solutions created/owned/stored by the User on or connected to Trinity Network facilities may subjected to inspection by the Director of IT Services or nominated agent. Should the data/software be encrypted the User shall be required to provide the decryption key to facilitate decryption of the data/programs. Where evidence is found of misuse or the illegal use of material it will be subject to removal/deletion.

A user's name, address, photograph, status, e-mail name, login name, alias, Staff/Student number and other related information will be stored in electronic form for use for administrative and other operational purposes.

Whilst the University takes appropriate security measures against unauthorised access to, alteration, disclosure, destruction, or accidental loss of personal and other data it cannot and does not give any warranties or undertakings to the user about security, confidentiality, or integrity of data, personal or other. The same applies to other IT material submitted to or processed on facilities provided or managed by the University or otherwise deposited at or left on its premises.

Other than any statutory obligation, the University will not be liable for any loss, damage or inconvenience arising directly or indirectly from the use of, or prevention of use of, any Network facility provided and/or managed by the University.

All Network Users must comply with the following conditions of use which apply to the Trinity network and all attached devices:

- Users should not use or produce materials or resources to facilitate unauthorised corruption, changes, malfunction or access to any Trinity or Network facilities.
- Users should not display, store or transmit content, images, or text which is illegal or could be considered offensive e.g., material of a sexual, pornographic, paedophilic, sexist, racist, libellous, threatening, defamatory nature, of a terrorist nature or likely to bring Trinity into disrepute.
- Users must not forge email signatures and/or headers, initiate and/or forward 'chain' or 'junk' or 'harassing' mail.
- Users must comply with all relevant IT legislation as outlined in the IT and Cyber Security Policy.
- When holding data on computers about living individuals, Users must register the data and its uses, according to Trinity procedures and in accordance with the General Data Protection Regulation.

Breaking these conditions may lead to Trinity disciplinary procedures being invoked, with penalties, which could include suspension from the use of all Trinity computing facilities for extended periods and or fines. Serious cases may lead to expulsion or dismissal from Trinity and may involve civil or criminal action being taken against the user.

13.2 Internet Use Policy

The Internet is recognised as an important communication and research tool for Trinity College network Users. This policy details standards for the secure use of Internet facilities for Trinity purposes, including teaching, research, and administration.

13.2.1 Conditions Governing use of Trinity Internet Facilities

All Users must adhere to the following when using College facilities to connect to the Internet:

- Access to the Internet is provided for Trinity College purposes and must not be abused for personal use.
- Commercial use, which is not connected to or approved by the University, is strictly prohibited and will result in disciplinary procedures,
- Internet access in Trinity campus locations is available only via the Trinity infrastructure. Users should not connect to the Internet via any other means on Trinity computers connected to the Trinity campus network.
- Users are expected to act ethically and responsibly in their use of the Internet and to comply with the relevant national legislation, the Trinity IT and Cyber Security Policy, regulations, and codes of practice. Users must not post messages on forums or websites which are likely to be considered abusive, offensive, or inflammatory by others.
- Users must not use the Trinity Internet connection to scan or attack other individuals/devices/organisations. The use of vulnerability scanners or other hacking tools unless used as part of an approved course of study is strictly prohibited.
- Users should be aware that the public nature of the Internet dictates that the confidentiality and integrity of information cannot normally be relied upon. Where a requirement exists to send or receive confidential or commercially sensitive data over the Internet, a security mechanism recommended by IT Services should be used.
- Passwords used for personal Internet services should not be the same or similar to passwords used for services accessed within Trinity. Similarly, any username used for the Internet services should not be the same or similar to a Trinity username. This is to prevent unauthorised access to Trinity resource occurring as a result of a breach of usernames and passwords held in another Internet service, social media etc.
- Software copyrights and licence conditions must be observed. Only licensed files or software may be downloaded from the Internet.
- The use of the Trinity Internet Connection to download or distribute copyright material using peer-to-peer applications is strictly prohibited. IT Services reserve the right to disconnect any machines involved in illegal file distribution from the Trinity network.
- All devices connected to the Internet must be equipped with the latest versions of anti-virus software, which has been both approved and supplied by Trinity.
- All forms of data received over the Internet should immediately be virus checked.
- All forms of data transmitted from Trinity over the Internet should be virus checked in advance.
- Data, which has been compressed or encrypted, should be decompressed, or decrypted as required before virus checking.
- All security incidents involving Internet access must be reported to IT Services.

13.3 Email and Messaging Use Policy

E-mail, Chat, Messaging and other forms of person-to-person digital communications is recognised as an important communication tool for Trinity College Users. This policy details standards for the secure use of email and other messaging services for Trinity purposes, including teaching, research, and administration.

13.3.1 Conditions governing use of Trinity E-mail and Messaging facilities

All Users must adhere to the following when using Trinity E-mail facilities:

- Users are expected to act ethically and responsibly in their use of e-mails and to comply with the relevant national legislation, the Trinity IT and Cyber Security Policy, regulations, and codes of practice.
- Discrimination, victimisation, or harassment on the grounds of gender, marital status, family status, sexual orientation, religious belief, age, disability, race, colour, nationality, ethnic or national origin is against Trinity Policy. Users must not bully, hassle, or harass other individuals via e-mail. Users must not send messages that are likely to be considered abusive, offensive, or inflammatory by the recipient/s.
- All Users should regard all e-mails sent from Trinity facilities as first, representing Trinity and, secondly, representing the individual. Users should be civil and courteous. Users should not send e-mail, which portrays Trinity in an unprofessional light. Trinity is liable for the opinions and communications of its staff and students. Any e-mail involved in a legal dispute may have to be produced as evidence in court.
- All Users should do their best to ensure that email content is accurate, factual, and objective especially in relation to individuals. Users should avoid subjective opinions about individuals or other organisations.
- Users should be aware that e-mails can easily be forwarded to other parties. Users should assume that anyone mentioned in e-mail could see it or hear about it or he/she may, under data protection or other law, be entitled to see it.
- All Users should be aware that. It is possible for the origin of an e-mail to be easily disguised and for it to appear to come from someone else.

  All Users must be vigilant for email fraud, including financial fraud, impersonation attempts and phishing. Users should exercise caution when accessing links contained in emails. Users should not supply their TCD username and password in response to links in email messages.
- Users must not use a false identity in e-mails.
- Users must not create or forward advertisements, chain letters or unsolicited e-mails e.g., SPAM.
- All Users should protect data displayed on their monitor or laptop screen. E.G by putting the laptop into 'sleep' mode, by locking their computer, by using a screen saver in password- protected mode when leaving their desk or by locking their office door if a single office occupancy.
- All Users should exercise caution when providing their e-mail address to others and be aware that their e-mail address may be recorded on the Internet.

- All Users should be cautious when opening e-mails and attachments from unknown sources as they may be infected with viruses.
- All Users must have up-to-date Trinity approved anti-virus software installed and operational on the computer that they access their email on.
- All emails or attachments that are encrypted or compressed should be decrypted or decompressed and scanned for viruses by the recipient.
- Email attachments should be encrypted to protect the content from unauthorised access. Email attachments containing personal or sensitive must always be encrypted. Users should be aware that e-mails may be subject to audit by IT Services to ensure that they meet the requirements of this policy. This applies to all message content, attachments, and addressees, and to personal e-mails.
- It is not permitted to automatically forward all emails to an external non-Trinity managed email account.
- As part of Trinity's standard computing practices, email systems and the systems involved in the transmission and storage of e-mail messages are "backed up" for administrative purposes. The frequency and retention of back-up copies vary from system to system. This back-up is for Trinity administrative purposes only and it is the User's own responsibility to back-up any of their e-mails they wish to retain for future reference.
- All security incidents involving e-mail should be reported to IT Services.

13.3.2 E-mail and the General Data Protection Regulation (GDPR)

All Trinity Users should be aware that e-mail containing information pertaining to living individuals fall under the scope of the General Data Protection Regulation (GDPR).

All Users must ensure that the methods of collecting, processing and storing information personal information via email comply with the Trinity policies the GDPR and any other relevant legislation.

13.3.3 E-mail and Privacy

Trinity Users must assume that all e-mail or Internet communications are not secure unless encrypted and they should not send via e-mail any information, which is confidential. All e-mails may be disclosed to third parties under Freedom of Information requests. Users may not, under any circumstances, monitor, and intercept or browse other Users' e-mail messages unless authorised to do so by the Director of IT Services. Network and computer operations personnel, or system administrators, may not monitor other Users' e-mail messages other than to the extent that this may occur incidentally in the normal course of their work.

The University reserves the right to access and disclose the contents of a User's e-mail messages, in accordance with its legal and audit obligations, and for legitimate operational purposes. Trinity reserves the right to demand that encryption keys, where used, be made available so that it can fulfil its right of access to a User's e-mail messages in such circumstances.

13.3.4 Chat and Messaging Services

The provisions and requirements for e-mail under sections 13.3.1 to 13.3.3 apply equally to Chat and other digital / online messaging and communications services, including social media.

13.4 Password Policy

Username and passwords are utilised in Trinity to facilitate access to Trinity IT resources. They also protect Trinity data from access from unauthorised individuals both internally (other staff students) and externally (hackers).

This policy applies to all Trinity Staff, Students, or Third parties who are issued with usernames and passwords for any Trinity IT System or device.

This policy applies to all username and password pairs on all devices, systems and applications that are part of the Trinity network that provide access to Trinity owned information.

13.4.1 Issue of accounts and passwords

All system and application accounts and passwords must be issued by IT Services or an Autonomous Network Manager. Once a password has been issued, full responsibility for that account and associated password passes to the User.

13.4.2 Password Sharing Prohibition

User passwords must not be shared with or disclosed to other Users.

13.4.3 Writing Passwords Down and Leaving Where Others Could Discover

Passwords must not be written down and left in a place where unauthorised persons might discover them.

13.4.4 Password Changes

Password changes must be made when requested in person by the appropriate individual or when requested by a trusted party as defined by IT Services. No exceptions to this policy are allowed.

13.4.5 Minimum Password Length

The length of passwords must always be checked automatically at the time that Users construct or select them. All IT systems must require passwords of at least eight (8) characters.

13.4.6 Complex Passwords Required

All computer system Users must choose passwords that cannot be easily guessed. For example, a car license plate number, a spouse’s name, or an address must not be used. This also means that passwords must not be a word found in the dictionary or some other part of speech. For example, proper names, places, and slang must not be used.

13.4.7 Cyclical Passwords Prohibited

Users must not construct passwords using a basic sequence of characters that is then partially changed based on the date or some other predictable factor. For example, Users must not employ passwords like “JANUARY” in January, “FEBRUARY” in February, etc.

13.4.8 User-Chosen Passwords Must Not Be Reused

Users must not construct passwords that are identical or substantially similar to passwords that they had previously employed.

13.4.9 Password Ageing

Passwords should be changed periodically. Network managers, system administrators or application administrators should select an appropriate time frame for changing passwords.

13.4.10 Limit on Consecutive Unsuccessful Attempts to Enter a Password

To prevent password guessing attacks, the number of consecutive attempts to enter an incorrect password must be strictly limited. After a defined number of unsuccessful attempts to enter a password (usually between 3and 8 per hour), the involved user account must be either (a) suspended until reset by a system administrator, (b) temporarily disabled for no less than three (3) minutes, or (c) if dial-up or other external network connections are involved, disconnected.

13.4.11 Password History

A password history must be maintained for all domain level. This history file should be used to prevent Users from reusing passwords. The history file should minimally contain the last 7 passwords for each username.

13.4.12 System Compromise

Whenever an unauthorised party has compromised a system, IT Services or the relevant Autonomous network manager or application administrator must immediately change every password on the involved system. Even suspicion of a compromise likewise requires that all passwords be changed immediately. Under either of these circumstances, a trusted version of the operating system and all security-related software must also be reloaded. Similarly, under either of these circumstances, all recent changes to user and system privileges must be reviewed for unauthorised modifications.

13.4.13 Storage of Passwords in Readable Form

Passwords must not be stored in readable form in batch files, automatic login scripts, software macros, terminal function keys, in computers without access control, or in other locations where unauthorised persons might discover them.

13.4.14 Changing Vendor Default Passwords

All vendor-supplied default passwords e.g., default passwords supplied with routers, switches, or software such as operating systems and databases must be changed before any computer or communications system is used.

13.4.15 Encryption

Passwords must always be encrypted when held in storage for any significant period of time or when transmitted over communications system.

13.4.16 Misuse of Passwords

Any abuse of passwords must be reported to IT Services who will advise on what follow-up action to take. Passwords must always be changed if it is known or suspected that another person has become aware of the password. Where a third party is found in possession of a User's password that account will be disabled. In this situation the valid User should report this to IT Services.

13.4.17 Multifactor Authentication

Multifactor authentication provides additional security by requiring a second identifying piece of information such as a code provided by text message to a mobile phone or via an Authenticator app.

Multi-factor authentication must be used in addition to a password for all University software solutions whether created/purchased/leased used in the storage or processing of university data.

13.5 Malware/Virus and Spam and Phishing Policy

Computer Malware/Viruses can impact productivity, University operations, incur a financial cost and can result in the compromise or loss of data and reputation.

Malware/Viruses can originate from a range of sources, spread rapidly, and require a comprehensive approach to ensure the risk they pose is effectively managed. This comprehensive approach requires the full co-operation of all Trinity College Staff and Students. This Anti-Virus and Anti-Spam Policy outlines the overall approach adopted by the Trinity as well as individual responsibilities.

All Trinity College network Users have a responsibility to protect University systems from malware / virus infection and must follow the guidelines on spam email as outlined below:

13.5.1 Malware / Virus Prevention – Network Users Responsibilities

All Users have a responsibility to protect any device they use which connects to the Trinity network by ensuring that they have the installed the correct anti-virus product for their area and that it is up to date. This relates to Trinity owned machines and User's private machines where the machines are used to access the Trinity network.

- Users must not try to install an unapproved anti-virus product or try to alter the configuration or disable the existing anti-virus product.
- Users must install when requested by IT Services or their Autonomous Network Manager any software, which is for the prevention of or monitoring of malware infections.
- Users must ensure that all relevant software security updates are applied to their computer. Users are advised to use the Windows update service for all Microsoft operating systems, and the equivalent update service for other types of operating system.
- Users must ensure their hard drives are scanned regularly for malware.
- Users should not open suspicious emails or attachments whether solicited or unsolicited from unknown or unusual sources.

- Users should scan all software or other content that they download from the Internet for viruses.
- Users should exercise caution when downloading software from the Internet and only install software from reputable Internet sites.

13.5.2 Where malware is detected by a User

- All Users must respond to any malware infection detection indicated by their anti-virus software.
- In the event that a User is unable to clean or remove an infected file they should disconnect their computer from the Trinity network by removing the network cable, turn off Wireless access and inform their Autonomous Network Manager or the IT Services Helpdesk of the problem immediately.
- All Users should be alert to the possibility of malware and report any suspicious behaviour to their Autonomous Network Manager or the IT Services Helpdesk immediately.

13.5.3 Unsolicited Email (Spam) User Responsibilities

- Users should exercise caution when divulging their Trinity Email account to third parties. Some organisations may provide your email address to parties involved in sending unsolicited emails (Spam), which may result in increased volumes of spam email being sent to your account.
- IT Services provide a Spam filtering service for users of the Trinity email system. All Users should report any spam that they receive using the method advised by IT Services in order to improve the overall efficiency of the system.

13.5.4 Phishing – User Responsibilities

- Phishing is a form of online fraud. In a typical phishing incident, a User may receive an email or pop-up message that claims to be from IT Services or another business or organisation that they may have previously dealt with.
- Trinity staff and students must treat any email that asks for their Trinity username and password details with extreme caution.
- Any User who suspects that they have fallen for a phishing attack and compromised their Trinity username and password must immediately change their password and inform IT Services.

13.5.5 Virus and spam Prevention – Administrative responsibilities

IT Services, and Autonomous Network managers must:

- Select an effective desktop anti-virus product. This product must be licensed and made available to all Users connecting to the Trinity network.
- Monitor systems regularly for devices that do not have anti-virus software installed or have incorrect anti-virus products or settings.

- Provide a central point of contact to Trinity Users for malware matters.
- Keep abreast of potential malware that may affect Trinity.
- Promote awareness of malware issues amongst Users.
- Monitor user endpoint systems for indications of malware infection using available tools.
- Follow up on and evaluate any malware reports from Users and make recommendations which may include informing Users of the problem by email alert, intranet, etc.
- During a malware outbreak incident, provide whatever assistance is required to disinfect the device and prevent propagation.
- In the event of an incident the official source of updated information will be the IT Services website.
- IT Services and Autonomous Network managers running approved Trinity email systems must scan all incoming and outgoing email at the mail gateway for viruses using a reputable malware scanning product. This is to prevent mass propagation of viruses through email systems.
- IT Services and Autonomous Network managers running approved Trinity email systems must offer a high-quality spam filtering service to all Users.

13.6 Software Security Policy

Software is widely used by Trinity College Dublin to process, manipulate, and store data owned by Trinity. It is essential that all software meet minimum-security standards to ensure the integrity and security of Trinity data.

This policy applies to all Trinity staff, students or third parties who purchase or develop software solutions that are used on the Trinity network or installed on any device connected to the Trinity network or used to collect, store or process Trinity data. This policy applies to all software purchased with private resources as well as Trinity funds.

Particular care should be taken when purchasing or developing a major system that is to be used to process or store Trinity data.

The responsibility for ensuring that software solutions meet security requirements falls to the individual or group purchasing installing and configuring the product.

Where an individual does not have the required expertise to ensure that the product meets requirements advice should be sought from IT Services.

13.6.1 Software Security Standards

All software solutions must comply with the following standards:

- All software solutions must protect Trinity and personal information from unauthorised disclosure (confidentiality and privacy).

- All software solutions must protect Trinity and personal information from unauthorised modification (integrity).
- All software solutions must protect Trinity and personal information and processing services from disruption and destruction (availability).
- All software solutions must contain controls that can ensure that individuals can be held responsible for their actions (accountability and non-repudiation).

13.6.2 Purchasing Software

Any Staff member, Student or Third party purchasing software to be used on the Trinity network or to process data owned by Trinity must ensure that:

- The software meets minimum standards as detailed in section 13.6.1
- The software is adequately tested to ensure that the security criteria as defined in section 13.6.1 are met.
- The software is configured correctly and securely and that all relevant security features are enabled.
- The software is appropriately procured and licensed in accordance with its use by or for Trinity.
- The licensing and copyright criteria as detailed in section 13.6.12 and 13.6.13 are met.
- That provision is made for providing ongoing maintenance for the software either by the manufacturer or a dedicated system administrator.
- Physical or logical access should only be given to vendors for support purposes when necessary. Only approved secure methods of access should be used. (The IT Security officer can advise on suitable methods) The vendor must sign a third-party access form and the vendors activities should be monitored/logged.

13.6.3 Purchasing/Using Cloud software systems

Cloud computing is a method of delivering Information and Communication Technology (ICT) services where the customer pays to use, rather than necessarily own, the resources. These services are typically provided by third parties using Internet technologies.

The processes involved in procuring and evaluating cloud services can be complex and subject to legal, ethical and policy compliance requirements. These requirements must be evaluated and met prior to signing up to and using cloud services. This is essential to ensure that personal, sensitive, and confidential business data and information owned, controlled, or processed by the College, its staff, students, and its agents is adequately protected at all times. The service must be configured and confirmed to ensure that the data and information is secure and that an adequate backup and recovery plan is in place to ensure that data and information can be retrieved to meet business needs. For more critical systems, the service should be built with high availability, again to meet business needs.

All procurement of Cloud services is subject to the University Cloud Policy copies of which can be obtained from the Trinity website or from IT Services.

13.6.4 Use of AI Software/Tools

Any Staff member, Student or Third party developing or purchasing or otherwise making use of Artificial Intelligence Software to be used on the Trinity network or to process data owned by Trinity must ensure that:

- All uses of generative AI software or tools to process or store confidential University Data are reviewed and approved by IT Services and the Data Protection Officer to ensure that confidential University data is not directly or indirectly disclosed, retained or used inappropriately by the provider of the AI Software or as a result of the use of the AI tools.

13.6.5 Software Development

Any Staff member, Student or Third party developing software to be used by Trinity or to process data owned by Trinity must ensure that:

- The software solution meets minimum standards as detailed in section 13.6.1.
- The software solution is tested a professional manner to ensure that all security controls are effective. Documentation supporting this must be made available to IT Services, or Network Manager on request.
- Software development and testing is carried out in a separate environment from the live environment.
- Adequate controls are in place over any test data, which is used in the testing process.
- That provision is made for ongoing maintenance of the software solution for the life of the solution.

13.6.6 Trinity Data

Any Staff member, Student or Third party purchasing or developing software for gathering, processing, or storing sensitive Trinity information such as financial data, sensitive teaching or research data or personal data relating to individuals must ensure:

- That the software meets the criteria as defined in section 13.6.1
- That they are able to provide documentation of security controls in place.

- That they are able to provide evidence of the effectiveness of those controls gained through proper testing exercises on request from IT Services or the relevant Network Manager or Systems administrator.
- Where sensitive data (E.G financial data, sensitive teaching or research data or personal data relating to individuals) is to be stored in electronic format that Trinity has insurance to cover any incident such as theft of the data, which may occur while the data is stored electronically.
- That they are not duplicating data already held in central Trinity databases (e.g., Student and Staff details) or creating systems which duplicate services already provided by existing systems.

13.6.7 E-Payment or Storage of Credit / Debit Card Numbers

Users intending to purchase or develop systems intended for e-payment or the collection and/or storing credit card numbers and associated information are alerted to the following special security considerations:

- Online payments may only be processed using University procured PCI compliant payment providers; further information is available from IT Services and the Financial Services Division.
- Payment card data must not be stored on the Trinity network or in University systems such as email.

13.6.8 Authentication

Software Solutions should use secure authentication methods utilising strong passwords and multi-factor authentication as a minimum.

13.6.9 Change Control

To minimise the corruption of information systems there should be strict control over the implementation of changes to software installations.

Where appropriate formal change control procedures should be enforced to ensure that security procedures are not compromised and that formal agreement and approval for any change is obtained. This should include:

- Authorisation of request for change.
- Risk assessment of change.
- User Acceptance Testing.
- Relevant management sign-off.
- Information Security sign-off.
- Rollback procedures in the event that the promotion failed.
- Documentation of the above

13.6.10 Encryption

- Sensitive data (E.G financial data, sensitive teaching or research data or personal data relating to individuals) to be transmitted over any external communication network, must be sent in encrypted form.
- It may also be appropriate to use encryption where sensitive data is transmitted internally across the Trinity network. In this case a risk assessment should be carried out to determine whether a cryptographic control is appropriate.
- If sensitive data is to be transported in portable media e.g., USB devices etc it must be in encrypted form.
- If encryption is used, the information protected with encryption must be transmitted over a different communication channel than the keys used to govern the encryption process.
- The owner(s) of data protected via encryption must explicitly assign responsibility for the encryption key management to be used to protect this data.
- Encryption should be used to protect data at rest. (database encryption)

13.6.11 Software Installation, Configuration and Updates

End users must ensure that they install and configure all software to a secure baseline standard. End users should ensure that they also install any updates or security patches that are available for the operating software application software or databases installed on devices connected to the Trinity network or which are used to process or store Trinity data.

All Network Managers, system administrators, database administrators and application administrators must ensure that they install and configure all software in a secure manner and that they install all updates or security patches on operating systems, applications, databases, and any other software, which they purchase, develop or administer.

Specific technical details on secure installation and configuration of operating systems and other software are available from the IT Services.

13.6.12 Licensing

All Network Managers, Area IT Support Representatives, database administrators and individuals are responsible for maintaining records of software licences for all software that they acquire.

Software that is acquired on a trial basis must be used in accordance with the vendor's copyright instructions.

13.6.13 Copyright

Copyright stipulations governing vendor-supplied software must be observed at all times. All software developed within Trinity is the property of Trinity and should not be copied or distributed without prior written authorisation.

13.6.14 Breach of Policy

Where software is found to be in breach of this policy, the Director of IT Services, or Network Manager may direct that the software system/application is withdrawn from live operation.

13.7 Data Backup Policy

Back-up procedures, ensuring that both data and software are regularly and securely backed-up, are essential to protect against the loss of that data and software and to facilitate a rapid recovery from any IT failure. This policy outlines guidelines for Trinity College staff and students on backing up Trinity Data.

The data backup element of this policy applies to all staff, students and third parties who use IT devices connected to the Trinity College network or who process, or store information owned by Trinity College Dublin.

All Users are responsible for arranging adequate data backup procedures for the data held on IT systems assigned to them.

13.7.1 Best Practice Backup Procedures

All backups must conform to the following best practice procedures:

- All data, applications, operating systems and utility files must be adequately and systematically backed up (Ensure this includes all patches, fixes and updates)
- Records of what is backed up and to where must be maintained.
- Records of software licensing should be backed up.
- Back-up media, together with the back-up record, should be stored safely in a remote location, at a sufficient distance away to escape any damage from a disaster at the main site.
- Regular tests of restoring data/software from the backup copies should be undertaken, to ensure that they can be relied upon for use in an emergency.

13.7.2 Responsibility for Data backup

Only critical systems are routinely backed up by IT Services and Autonomous Network Managers in the current model. The responsibility for backing up data held on the endpoint systems (laptops, tablets, phones, removable devices) of individuals regardless of whether they are owned privately or by the University falls entirely to the owner or operator of those systems.

Users responsible for a collection of data held either remotely on a server or on the hard disk of a computer, should consult their Autonomous Network Manager or IT Services about local back-up procedures.

Users who do not use the facilities provided by IT Services or those of their own academic or administrative area should put in place their own procedures.

13.7.3 Legal Requirements

Users when formulating a backup strategy should take the following legal implications into consideration:

- Where data held is personal data within the meaning of the General Data Protection Regulation (GDPR), there is a legal requirement to ensure that such back-ups are adequate for the purpose of protecting that data.
- Depending on legal or other requirements, e.g., Financial Regulations, it may be necessary to retain essential business data for a number of years and for some archive copies to be permanently retained.
- Depending on legal or other requirements, e.g., General Data Protection Regulation (GDPR), Software Licensing, it may be necessary to destroy all backup copies of data after a certain period or at the end of a contract.

13.7.4 User Backups

The responsibility for backing up data held on the endpoint systems (laptops, tablets, phones, removeable devices) of individuals regardless of whether they are owned privately or by the College falls entirely to the owner or operator of those systems.

All network Users should ensure that their data is backed up using one or a combination of the following methods:

- Backing up data to an IT Services recommended service e.g., Microsoft OneDrive.
- Backing-up to a local storage device e.g., removable disk
- Copying critical data on a regular basis to a server that is properly backed up by the College.
- Backups should be scheduled regularly.
- All Users should backup their data before updating or upgrading software on their endpoint systems.

13.8 Disaster Recovery Policy

The disaster recovery procedures in this policy apply to IT Services, Autonomous Networks and all Trinity Users who are responsible for systems or for a collection of data held either remotely on a server or on the hard disk of a computer.

13.8.1 Published Disaster Recovery Plan/Procedures

- Trinity must develop, maintain, publish and test a Disaster recovery plan.
- IT Services and Autonomous Network managers must contribute details of data/systems owned or managed by them and the plans procedures for disaster recovery annually.
- IT Services and Autonomous Network managers must regularly schedule regular testing of the Disaster recovery plan or parts thereof.

13.8.2 User Responsibilities

All Trinity Users should make preparation for a disaster event in which IT equipment or data is destroyed. Users should:

- Ensure that they have backup up all important data stored on equipment owned by or assigned to them. IT Services or an Autonomous Network manager can provide detailed advice on how best to achieve this.
- Note the procedures for procuring replacement hardware. This can be done by purchasing it from a suitable hardware vendor or by using spare capacity on a colleague's computer in another building/site.
- Maintain backup documentation regarding any licence keys that they may hold.

13.8.3 Best Practice Disaster Recovery Procedures

A disaster recovery plan can be defined as the on-going process of planning developing and implementing disaster recovery management procedures and processes to ensure the efficient and effective resumption of vital Trinity functions in the event of an unscheduled interruption.

All disaster recovery plans must contain the following key elements:

- Critical Application Assessment
- Backup Procedures
- Recovery Procedures
- Implementation Procedures
- Test Procedures
- Plan Maintenance

13.9 Remote Access Policy

The purpose of this policy is to define standards for connecting to the Trinity College Network from a Computer or other device located outside of the Trinity network. This policy is designed to minimise the potential exposure to Trinity from risks associated with remote access connections by ensuring only secure methods are used to connect to the Trinity network.

This policy applies to all Trinity Staff, students or Third parties with either a Trinity owned or personally owned computer used to connect to the Trinity network.

13.9.1 Permitted remote access connections

Remote access connections to the Trinity network may be made for Trinity administrative or academic purposes only. These include but are not limited to:

- Approved use of network resources service by registered Staff and Students.
- Remote or Hybrid working by registered Trinity Staff.
- Network administration purposes by registered System Administration Staff.
- Administration of Trinity Applications or Systems by approved Third parties.

13.9.2 Methods of Remote connection

IT Services and Autonomous network managers only may approve appropriate remote access technologies for use to access the Trinity network.

Trinity Users should apply to IT Services or the Autonomous network managers for a list of currently approved methods.

Current preferred remote access technologies include but are not limited to:

- Approved university or AMN Virtual private network (VPN)
- Secured access via the University border firewalls as approved by IT Services

13.9.3 Non-standard remote access connections

Organisations or individuals wishing to implement non-standard Remote Access must obtain prior written approval from IT Services.

13.9.4 Protecting Remote Access Credentials

All individuals are responsible for safeguarding the remote access credentials granted to them and making sure that unauthorised individuals do not use them. These credentials may consist of username and password combinations, digital certificates or other software or hardware.

13.9.5 Authentication

Where Username/Password authentication is used the following apply:

- Where remote access authentication is facilitated using a username and password a strong password must be used as defined in the password policy
- Multifactor authentication must be utilised.
- At no time should any Trinity staff member or student provide their username or password to any unauthorised third party.

13.9.6 Remote Access Hosts

All hosts that are used for remote access to the Trinity network or by Trinity staff to process University data remotely must:

- Be managed in accordance with the latest guidance from IT Services
- Use the most up-to-date anti-virus software.
- Be protected by a Trinity or private Firewall.
- Be kept physically safe and secure in a suitable location where they cannot be accessed by unauthorised individuals.
- Not be made available for use to unauthorised third parties.
- Be available for inspection by IT Services or the Autonomous Network Manager/Administrator if requested.

13.9.7 All Individuals/groups granted remote access connection privileges

It is the responsibility of all individuals/groups with remote access privileges to the Trinity network to ensure that:

- Their remote access connection meets security standards as approved by the University.
- The connection is only used for approved purposes.
- The remote access credentials granted to them are held safely and not disclosed to unauthorised third parties.

13.9.8 Trinity Staff or Students providing remote access to Third parties

Trinity staff or students may only provide remote access to the Trinity network to third parties with the express permission of IT Services or Network Manager.

Trinity Staff providing remote access to third parties for any purpose must ensure that the method of remote access meets security standards as approved by the University.

The Third party must be made aware of their responsibilities to comply with this policy.

Details of the Third-Party connection must be documented and submitted to the Autonomous Network Manager/Administrator and to IT Services.

13.9.9 Third Parties

It is the responsibility of all contractors, vendors and agents with remote access privileges to the Trinity network to ensure that the remote access connection adheres to the Security Standards as defined in this policy.

All Third parties must comply with the security measures as outlined in this policy document.

13.10 Third Party Access Policy

The purpose of this policy is to define standards for all Third Parties seeking to access the Trinity Network or any devices attached to the Trinity Network. This policy is designed to minimise the potential exposure to the Trinity from risks associated with Third Party Access.

13.10.1 Scope

This policy applies to all Trinity Staff, students seeking to provide access to the Trinity network or devices attached to the network to Third parties.

13.10.2 Permitted Third Party Access

Third party access to the University network may be made for administrative or academic purposes only.

13.10.3 Access Requests

Requests to allow access to the Trinity network or attached devices must meet the following criteria:

- Requests for third party access must be formally authorised in writing by IT Services or the relevant Autonomous Network Manager for the area prior to access being granted.
- The requester acts as the sponsor for the Third Party and take responsibility for the actions of the Third Party when accessing the College network or attached devices.
- Where there is an approved need for third party access, security controls will be agreed and defined in a contract with the third party as per 13.10.4
- Access to Trinity College network facilities by third parties will not be provided until the appropriate measures have been implemented and a contract signed defining the terms for the connection.
- Third party access must be permitted only to the facilities, services and data, which are required to perform the specified tasks, as outlined to the Network Manager/Administrator in the original request for access.

13.10.4 Security Conditions in Third Party contracts

Third party access to Trinity IT facilities must be based on a formal contract, which must address the following issues:

- A description of each facility, IT service or type of data to be made available must be included.
- Compliance with the published Trinity IT and Cyber Security Policy.
- Permitted access methods and the control and use of unique identifiers (User Ids) and passwords.
- A requirement to maintain a list of individuals authorised to use the service.
- A commitment such that all Third Party’s granted access will inform the College in writing of staff changes that affect the integrity of security. This includes the rotation and resignation of employees so that the College can disable userids and remove / change passwords in order to secure its resources.
- Procedures regarding protection of Trinity assets, including information.
- Responsibilities with respect to legislation including but not limited to the General Data Protection Regulation (GDPR)
- The right of Trinity to monitor User activity and revoke access.
- Responsibilities regarding hardware and software installation and maintenance.
- The right to audit contractual responsibilities.
- Restrictions on copying and disclosing information.
- Measures to ensure the return or destruction of information at the end of the contract.
- Any required physical protection measures.
- Measures to ensure protection against the spread of computer viruses.

- An acknowledgement that accesses to Trinity systems and information will be granted for approved purposes only. The use of this access for personal use or gain is strictly prohibited.
- Arrangements for reporting and investigating security incidents.

13.10.5 Unique Authentication

To ensure individual accountability on Trinity Network devices and applications, all third parties granted access must be given a unique userid and password.

The third party will always be held responsible for any activities which occur on Trinity networks and applications using this unique userid.

The Third Party is solely responsible for ensuring that any username and password that they are granted remains confidential and is not used by unauthorised individuals.

13.10.6 Host Security

When a Third Party is logged into the Trinity network, they must not leave the host they are logged onto unattended.

Devices that are used to display Trinity data should be located in such a way that confidential information is not displayed to unauthorised persons or the general public.

Up-to-date Virus checking software must be installed on any relevant devices that are being used to access the Trinity Network or attached devices.

13.10.7 Remote Access by Third Parties

Where the type of access to be granted to the Network is from a remote device the third party must comply with the security measures as defined in this policy.

13.11 Incident Response and Misuse of IT Facilities Policy

In the event of a security incident occurring, it is important that all Trinity employees and students are aware of their responsibilities and the procedure by which incidents can be most effectively and efficiently brought to a satisfactory conclusion. The procedures as defined below are required practice within Trinity College.

Where investigation of a security incident indicates misuse of IT facilities approved disciplinary procedures will be implemented as defined in this policy.

13.11.1 Incident Reporting

The types of incidents that must be reported include, but are not limited to:

- Incidents reported from Systems and Networks (system failures, unusual activity)
- Anomalous events (unusual or suspicious behaviour noted in logs or activity reports)
- Reports from External sources (threats, customer queries, complaints, press reports)
- Incidents observed by network Users (on local PC’s or servers)
- Any unauthorised access to Trinity Data or systems.

13.11.2 Reporting an incident

All observed, reported, detected or suspected security incidents; vulnerabilities, weaknesses or threats must be reported to an Autonomous Network Manager, and /or IT Services immediately.

In no instance should any User attempt to prove a suspected weakness as this could lead to a potential misuse of the system. Where Users note that any software does not appear to be working correctly, i.e. according to specification, they should report the matter to IT Services.

Where a User suspects that the malfunction is due to a malicious piece of software e.g. a computer virus, they should stop using the computer, disconnect it from the Trinity network and report the matter to IT Services.

13.11.3 Disabling Accounts/Network Connections

IT Services and Autonomous Network Managers may disable User accounts and/or network connections:

- Pending investigation of a security incident or where investigation of an incident
- To contain a confirmed security breach and prevent other Trinity network devices from becoming affected by the incident.

13.11.4 Records of Security Incidents

IT Services will collate and analyse records of security incidents and will report to the Trinity Board or Board committees and University Leadership on any trends which emerge and recommend any additional action which should be taken University wide to try to prevent their occurrence in the future.

13.11.5 Misuse of facilities

Where Trinity Staff or Third parties are found to have misused Trinity IT facilities the Director, IT Services, Network Manager, or their nominated agent will inform the appropriate Trinity authorities who will determine what further action should be taken.

Where students are found to have misused Trinity IT facilities, IT Services must inform the Junior Dean who will determine what further action should be taken.

13.12 Legal Compliance Guidelines

The University has an obligation to abide by all Irish legislation and relevant legislation of the European Community.

All Users of the Trinity Information Systems must ensure that they are fully aware of and understand any of the relevant legislation, which applies to IT systems or data, assigned to them.

This Guideline is not a full statement of the law but is an indication of the issues to be complied with when processing information and disseminating it through the Trinity Information Systems.

13.12.1 Relevant legislation

Full copies of the legislation outlined below are available from the Trinity library and IT Services

- Regulation on Artificial Intelligence (AI Act)
- The General Data Protection Regulation (EU) 2016/679 (GDPR)
- Data Protection Act 2018
- The eprivacy regulations 2011 S.I. No.336 of 2011
- Data Protection Act 2018 (Section 36(2)) (Health Research Regulations)
- Criminal Damages Act (1991) revised 2019
- Child Trafficking and Pornography (Amendment) Act 2004
- Intellectual Property Miscellaneous Provisions Act (2014)
- Copyright and Related Rights Act (2000)
- S.I. No. 59/2012 - European Union (Copyright and Related Rights) Regulations 2012.
- Safety, Health and Welfare at Work Act 2005 (as amended) Non-Fatal Offences Against the Person Act (Revised 2023)
- Electronic Commerce Act (2000)
- ECommerce Directive (2000/31/EC)
- Regulations entitled European Communities (Directive 2000/31/EC) Regulations 2003 (S.I. No. 68 of 2003)
- Criminal Justice Act 2011
- Criminal Justice (Offences relating to Information Systems) Act 2017
- Freedom Of Information Act 2014

14. Document Control for Revised Policies

14.1 Date of initial approval: 9 July 2003

14.2 Date revised policy approved: 3 May 2018

14.3 Date policy effective from: 19 June 2024

14.4 Date of next review: Academic Year 2026/2027