EXCELSIA COLLEGE
Sydney

ICT FRAMEWORK

ICT-01

Objects of Excelsia College

Motivated by the Christian faith, as expressed by the Apostles' Creed and Nicene Creed, with fidelity to the Scriptures as the Word of God, the objects of the College are the advancement of the Christian faith and higher education.

1 Policy statement and principles

Excelsia College seeks to provide its authorised users with secure and timely access to information and communications technology (ICT) services and equipment to facilitate learning and teaching, research and innovation, engagement and other functions of the College.

This framework is intended to:

- provide a clear statement of responsibilities for all authorised users of College ICT services, including what constitutes acceptable and unacceptable use
- outline the provision, modification and removal of access to College ICT services
- express the commitment of the College to maintaining secure, effective and reliable College ICT services
- ensure that the equipment provided reflects the varying requirements of different positions, including but not limited to, staff and students working or studying remotely
- ensure provision of specialised or non-standard equipment to staff and, where applicable, students with disability
- define those who have authority to access various ICT systems of the College that require identity management (usually involving usernames and passwords) and those who will manage the processes of adding, changing, suspending and deactivating their access.

The College's approach to this policy framework is guided by the following principles.

1.1 Acceptable use of ICT services

i. The College is committed to ensuring the provision of a fair, safe and productive computing environment for the College community, by establishing clear responsibilities for authorised users that do not adversely impact the College's operations, assets or reputation.

ii. All authorised users must act in accordance with this policy and all other applicable College policies and procedures.

iii. College ICT services span multiple legal jurisdictions. Authorised users have a personal responsibility to be aware of the jurisdiction that applies to their location when using College ICT services.

iv. Authorised users are permitted to use College ICT services for properly authorised and supervised business, education or research purposes, providing that the use:

   a. is lawful
   b. is in a responsible, ethical and equitable manner
   c. is consistent with the values of the College as outlined in the College's codes of conduct
   d. does not create an intimidating or hostile work or study environment for others
   e. does not jeopardise the provision of a fair, safe and productive computing environment, and
   f. does not adversely impact the College's operations, assets or reputation.

v. Authorised users who are unsure whether a proposed use is permitted or authorised should seek written approval from their supervisor or Head of Department.

vi. College ICT services must not be used in any manner that the College considers to be inappropriate. This may include, but is not limited to:

   a. accessing pornography

   b. unauthorised monitoring of electronic communications

   c. knowingly downloading, storing, distributing or viewing of offensive, obscene, indecent, or menacing material. This could include, but is not limited to, defamatory material, material that could constitute racial or religious vilification, discriminatory material, material that incorporates gratuitous violence or frequent and highlighted bad language

   d. stalking, blackmailing or engaging in otherwise threatening behaviour

   e. any use which breaches a law, including copyright breaches, fraudulent activity, computer crimes and other computer offences

   f. transmitting spam or other unsolicited communications

   g. the introduction or distribution of security threats, including a virus or other harmful malware.

vii. Limited personal use of College ICT services is acceptable, providing that such use is otherwise in accordance with this policy. Limited personal use of College ICT services is a privilege which can be removed if found being abused.

viii. Authorised users must not tamper with College ICT services that may potentially cause performance degradation, service instability, or compromise operational efficiency, security or fair use.

ix. All equipment is property of the College and must be returned on termination of each engagement.

1.2 Authorised access and restriction

i. All authorised users are permitted to access the College ICT services, at a level commensurate with their position, role, delegated authority or student status.

ii. Access to all College ICT services will be removed when the relationship between authorised users and the College ceases.

iii. Authorised users must not use their access to College ICT services to gain inappropriate personal, academic, financial or other advantage.

iv. Authorised users must maintain the confidentiality of any personal information accessed via College ICT Services.

v. Authorised users must not attempt to gain unauthorised access to College ICT services (and the information stored thereon) to which they have not been given access, or permit others to do so.

vi. Authorised users of College ICT services are not permitted to provide others with their authentication credential(s). It is the responsibility of authorised users to ensure that their authentication credentials are securely stored as they are responsible for all activities initiated from their account or with their authentication credential(s).

1.3 Software licences

i. Software purchased by the College is licensed primarily to the College, however approval may be granted to authorised users for use at home or other locations on non-College owned computers during the course of work or study with the College.

   a. Authorised users must discontinue use and un-install the software from non-College owned computing device(s) upon cessation or termination of employment or completion of study, or upon notification by the College of its termination of the software license agreement.

ii. Authorised users must comply with contractual obligations and terms and conditions of use stated in the software license agreements entered by the College.

1.4 Monitoring and privacy

i. College ICT services are the property of the College. Anything sent or received using the network, systems and facilities of the College will therefore be transmitted and stored on College property (or on third party property on behalf of the College).

ii. The College reserves the right to monitor, access, log and analyse the activities of authorised users, and of College ICT services, and conduct reviews and audits as necessary.

iii. The College reserves the right to block or filter any use that breaches this Policy or exceeds the College's acceptable level of risk.

iv. Disclosure outside the College of any personal information or contents of electronic communications must be in accordance with any relevant legislation, not limited to the *Privacy Act 1988 (Cth), Privacy and Personal Information Protection Act 1998 No 133* (NSW), the *Government Information (Public Access) Act 2009* (NSW), the *Health Records and Information Privacy Act 2002 No 71* (NSW), and the College's Privacy Policy in the Information Management and Privacy Framework.

v. The College may take any action deemed necessary to remedy immediate threats to College ICT services or information and communications technology security including, without limitation, suspending an authorised user's access, confiscation of College owned electronic devices and/or disconnecting or disabling equipment with or without prior notice.

1.5 Procurement/Lease of equipment

i. All equipment must be acquired through purchase or lease by the Finance and Administration Department and remains the property or custody of the College. Any request for equipment must be submitted in accordance with the published Financial and Administration – Staff Framework.

ii. All equipment requests and purchases are subject to the final approval of the Finance and Administration Department. A request may be declined for any of the below reasons:

   a. The requested equipment does not meet the guidelines contained within this policy.

   b. The requested equipment is not appropriate for the College technical environment.

   c. There are insufficient funds available to purchase the requested equipment.

   d. The requested equipment is not appropriate for the specified purpose.

   e. The equipment does not meet an identified business requirement.

1.6 Staff allocation of equipment

1.6.1 Standard allocation

i. As a general principle, a wireless headset, laptop computer, second monitor, keyboard and mouse will be provided for each established position within the College.

ii. Contractors, volunteers (including student placements) or other staff employed on a temporary basis who are not assigned to an established position may be assigned a computer on request for the period of their employment. The allocated computer must be returned to the Finance and Administration Department once the individual ceases to work at the College. Alternative arrangements may be made for remote locations where shipping of computers is not feasible.

1.6.2 Non-standard allocation

i. Any equipment outside of the standard allocation is discretionary and subject to available funding. Staff requiring any other equipment must submit a request to the Chief Financial Officer or Chief Operating Officer.

ii. Non-standard equipment is only allocated to staff that have a specific, direct need for this equipment when carrying out their day-to-day duties. All requests will be considered by the Finance and Administration Department and subject to the conditions contained within this policy.

iii. Non-standard equipment is allocated to a staff member for the duration of their employment in the position for which they requested use of the equipment. If the staff member is transferred to another position within the organisation, the staff member will need to submit a new request if they still require access to non-standard equipment.

iv. Usage of all non-standard equipment will be reviewed by the Finance and Administration Department on a regular basis and the equipment may be removed and reallocated where insufficient usage indicates that the position does not require permanent allocation.

1.6.3 Mobile phones

i. Excelsia do not provide any mobile phone for staff use. All staff members may communicate with fellow staff and students using the Teams app on their private phones without revealing their private numbers. They may communicate with external customers and stakeholders when they are assigned with a phone number or on a call queue established for the purposes.

1.6.4 Return of equipment

i. All equipment allocated to an individual must be returned to the Finance and Administration Department when the staff member:

   a. ceases employment with Excelsia College

   b. goes on leave for a period of eight weeks or longer

ii. It is the staff member and their manager's responsibility to ensure that all equipment issued is returned, including the device itself as well as any accessories which are allocated with it.

iii. The Finance and Administration Department may also request the return of equipment where usage audits indicate that the equipment is not being sufficiently utilised to warrant its ongoing allocation.

1.7 Compliance

i. Finance and Administration Department may provide regular reports to Management Committee on the usage of IT equipment.

1.8 Staff systems access management

i. The College is committed to ensuring that all staff who ought to have access to systems do so, in order to optimise staff productivity and the efficiency of the College.

ii. The College is committed to ensuring no one who ought not to have access to systems does so, in order to provide security for systems of the College and protect the privacy of its staff and students.

iii. The College is committed to ensuring that future options for systems access are not impeded by present decisions regarding ICT, particularly around usernames and passwords, in order to allow for continuous improvement.

1.9 Consequences of breach

i. Breaches of this Policy may be grounds for misconduct/serious misconduct.

ii. Without limiting Clause i, a breach or alleged breach of this Policy may result in a referral of the matter to the police and/or other relevant external authority.

iii. Without limiting Clause i, the Chief Financial Officer may immediately suspend an Authorised User's account in the case of a breach or an alleged breach of this Policy.

Non-compliance with this policy framework may result in disciplinary action in accordance with Excelsia College by-laws.

2 Scope

i. This Framework applies to all authorised users of the College ICT services managed by the College or third-party providers on behalf of the College, both on and off campus.

ii. This policy applies to all equipment issued and owned by the College. Devices covered by this policy include, but are not limited to, desktop computers, laptop computers, tablet devices, headsets, telephones, mobile phones, monitors and projectors.

3 Roles and responsibilities

The following stakeholders have a responsibility in relation to this policy framework.

Role	Responsibility
Chief Financial Officer	• Storage, version control, and scheduled review of this policy framework • Monitoring the effectiveness of this policy framework within their scope of responsibility • Making recommendations with respect to this policy to appropriate personnel and committees
Chief Global Engagement and Partnerships	• Managing Zoho One
Director of People and Culture	• Managing new and departing staff • Managing PeopleStreme
IT Manager	• Efficient allocation of equipment requested in accordance with this policy framework

	• Efficient assessment of any requests for equipment and providing appropriate advice where a request is refused • Procurement, deployment and disposal of College-owned equipment • Leasing, deployment and return-to-financial-provider of College-leased equipment • Ensuring that equipment is correctly configured for use • Ensuring equipment and associated software is adequately maintained/updated • Ensuring that authorised users are provided with information to utilise the equipment provided to them • Managing network and internet access, Microsoft 365 (including email), SharePoint, telephony (Teams Voice), printing (with PaperCut), Single-Sign-On, and ICT security, Excelsia Project and Workflow (Asana)
Heads of School and Departments	• Managing current staff • Appropriate management of pooled equipment • Ensuring that any items allocated to an individual are returned to the Finance and Administration Department prior to that individual leaving the College, including all accessories such as chargers, bags, cables etc. This also applies to any staff going on: o leave for a period of 8 weeks or more, or o secondment for any period.
Marketing Specialist	• Managing website SEO (Google Analytics, Brand 24)
Lead Designer	• Managing College information websites
Registrar	• Managing Student Management System (Paradigm), Learning Management System (Exo), Helpdesk (Zendesk)
Library Manager	• Managing Library Management (Liberty), Library e-Resources (Summon and EZproxy)
Staff	All staff are personally accountable in their use of work resources and are responsible for the equipment assigned to them individually or to their position: • Ensuring that all items are used in accordance with College policies • Ensuring that all items issued are kept secure within and when taken from College premises • Ensuring that equipment is not used by non-College individuals • Complying with any College ICT services requests to update equipment or software on that equipment • Complying with any requests to return equipment to the Finance and Administration Department • Informing the Finance and Administration Department immediately of any issues including damage, loss or theft of equipment

	• Ensuring efficient and proper use and care of equipment • Adhering to the requirements of this policy framework and any associated policies, guidelines or procedures

4 Definitions

For the purpose of this policy framework, the following definitions apply.

Term	Definition
action	There are four types of action regarding staff systems access: add, change, suspend and delete. • Add: To add a new staff member to the system. • Change: To change, usually increase, the number of systems a staff member can access. • Suspend: To deactivate, usually because of extended leave. • Delete: To remove a departing staff member from all the systems.
authentication credential	User identification and password, username and passcode, PINs or other confidential means used to gain access to College ICT services.
authorised user	All students, employees, contractors, consultants, temporary and other workers, including all personnel affiliated with third parties that use equipment owned by the College.
College ICT services	Facilities and services provided to an authorised user including software, communication devices and computing infrastructure under the control of the College (or a third-party provider on behalf of the College behalf) that provides access to information online or in electronic format.
IT equipment ('equipment')	Any device purchased/leased by Finance and Administration Department and in the custody of the College, including, but not limited to: • desktop computers • laptop computers • tablet devices • smart phones • desk telephones • projectors • peripheral devices including webcams, headsets, barcode scanners and multi-port hubs adapters.
personal information	Information or an opinion, regardless of its truthfulness and recording format or media, about an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion.

requester	Regarding staff systems access, there are two types of requesters: People and Culture; and all other Heads of Departments and Schools. • People and Culture can request two actions: add and delete. • Heads of Departments and Schools can request two actions: change and suspend.
system access management (staff) request	The request raised by the responsible parties regarding staff system access management.

5 Procedures

5.1 Staff systems access management

5.1.1 System managers

- IT Manager
    - Network and internet access: LAN and Wi-Fi with Internet access
    - Microsoft 365access: Excelsia Microsoft 365 with email (all staff and students) at domains excelsia.edu.au and student.excelsia.edu.au, respectively
    - Document Libraries on SharePoint Online and Teams groups
    - Telephony: Teams Voice (call queues, phone numbers)
    - Printing: office printing and Papercut utility
    - Asana: project management utility
    - Authentication: multi-factor authentication and Single Sign-On with other systems.

- Registrar
    - Paradigm: Student Management System
    - Totara (ExO): Learning Management System
    - Zendesk: support and ticket system for managing issues raised by students and academic staff in relation to courses and units
    - Acuity Scheduling, Booker and Timetabler: Room Booking System and course timetable scheduling system
- Chief Global Engagement and Partnerships
    - Zoho One

- Director of People and Culture
    - HR system

- Chief Finance Officer
    - Payroll System
    - Finance System

- Lead Designer
    - Excelsia College information website and associated websites

- Marketing Specialist
    - Google Analytics, Brand 24

5.1.2 Raising a staff system access request

A staff system access request must be emailed to it@excelsia.edu.au by the Heads of Department/Schools or their delegates; or otherwise from the People and Culture Department in the case of new employees or contractors.

5.2 Internal IT Help Desk

The primary role of the Internal IT Help Desk is to support end users in completing business tasks. In order to ensure this role is carried out in a timely and high-quality manner, a procedure has been established to help assign priority levels to problems or issues reported by end users to the IT Help Desk.

5.2.1 General guidelines for users needing help

i. To contact the IT Help Desk, email it@excelsia.edu.au or call the IT Helpline on (02) 9000 9634 to log a support ticket.

ii. Before contacting the Help Desk, try the following:

   a. If data loss isn't a concern, reboot your system if possible.

   b. Try to find a resolution to the problem yourself by reviewing available documentation, help sheets, and posted FAQs for the system that is presenting problems.

iii. Incidents and requests within a specific priority category will be handled on a first come, first served basis.

iv. In some cases, special consideration will be given to mobile and remote employees whose access to College resources is more constrained.

v. In the event of a natural disaster, failure of a third-party utility (such as electrical power failure), or some other catastrophic event, stated response and resolution times may be longer.

5.2.2 Incident priority levels for business systems serviced by a third-party

The following table shows different priority levels for incidents, response time and resolution time for business systems that are serviced by a third-party.

Severity	Description	Response Time	Resolution Time
Level 1	Critical system is down. Functions not usable. No workaround or alternative is available. Data is corrupted. Many end users are affected. Regulatory/legal deadlines will be missed.	15 minutes	1 hour
Level 2	Some functions are usable with severe restrictions. No workaround or alternative is available. Several end users affected.	1 hour	4 hours

Level 3	Basic functions are usable with minor restrictions. Workaround or alternative is available. One or more users affected.	4 hours	Next business day
Level 4	Minor problem. Functions are usable. Defect is cosmetic or simply a nuisance.	Next business day	5 business days

5.2.3 Reporting an incident

To report an incident, contact the Internal IT Help Desk at it@excelsia.edu.au or (02) 9000 9634. The IT Services Team will identify the concerned systems and assess the incident severity, and direct the incident to the right team if the concerned systems are not managed by the IT Services Team.

5.2.4 Submitting a service request

To submit a service request, fill out the online form at https://excelsia.zendesk.com/hc/en-us/requests/new. Alternatively, send your request details to it@excelsia.edu.au.

If the request is a new service or system at the College, prepare the business case for initial discussion with the IT Manager and/or the Chief Financial Officer. Official business proposals will require Management Committee approval for project initiation.

6 Student guidelines for use of IT systems

While studying at Excelsia College, there are a number of technologies that you will need to be familiar with. These guidelines do not exempt students from any other conditions of use that may be imposed by third-party suppliers of software.

6.1 Information website

The Excelsia College website is found at https://excelsia.edu.au

From the website, you can navigate to:

- the Excelsia College online learning portal, ExO
- the College Library
- course timetables
- course information, including course brochures
- College policies and procedures
- campus news
- wellbeing and safety information, where you can
    - report a hazard or incident

- report sexual assault or sexual harassment

- student support services such as
  - career support
  - counselling
  - academic skills
  - disability support.

6.2 Microsoft 365 and email

Microsoft 365 and access to your email can be found at: https://www.office.com

As an Excelsia student, you can access the full suite of Microsoft 365 applications including a student email account. The email account will be the primary means of official communication during your studies at Excelsia that you must visit frequently.

As a student, it is assumed you understand and have agreed to the terms and conditions of use for Microsoft 365 email (see section 7).

6.3 Excelsia Online (ExO)

You can access ExO through https://learn.excelsia.edu.au

Alternatively, you can access it via Excelsia College website (https://excelsia.edu.au), Current Students, then Excelsia Online (ExO).

Courses are administered via ExO where you can access:

- your enrolled units
- course unit outlines
- electronic assignment submission
- course unit evaluations
- library resources
- your student email (Microsoft 365).

6.4 My Enrolment (Paradigm)

To access Paradigm:

1. Go to the Excelsia College website (https://excelsia.edu.au)
2. Select 'Current Students' then Excelsia Online (ExO).

Once you are signed in to ExO using Microsoft 365, select 'Useful Links' to access 'My Enrolment (Paradigm)'.

6.5 Library catalogue portal

To access electronic library resources, go to the Excelsia website (Current Students page) or log in to ExO and select 'Library'. Then select 'Summon' and sign in with your student ID and Microsoft 365 password.

6.6 Internet access

You can access the internet via the wi-fi (wireless) connection on campus. Connect to the Excelsia-student wi-fi using your student ID and Microsoft 365 password. Alternatively, you can get the latest passcode at Reception for the Excelsia-guest wi-fi connection.

7 Terms and conditions for use of Microsoft 365 at Excelsia

All students are assumed to have agreed to these terms of use before commencing their studies.

Students understand and agree that:

- an Excelsia student email account is the means by which all official Excelsia College information will be communicated
- if a student is denied access to Excelsia Microsoft 365 due to legal reasons, they will be notified of the reason and hard copy of all communications will be issued instead
- Microsoft 365 accounts will be terminated upon graduation, withdrawal from a course, exceeding an approved leave of absence (after one year), failure to return to study (after one year), if enrolment or continuity in a course is withheld by the College as disciplinary action, or upon breach of these guidelines.

Breaches of these terms and conditions will be referred to the College's Academic Misconduct Committee. Sanctions may include suspension or removal of the Microsoft 365 access, suspension or expulsion from the College, and/or criminal or civil action.

The College will cooperate with any law enforcement agencies in the investigation of any illegal activities conducted on its communications systems, and will release requested emails for the purpose of an investigation.

In relation to Microsoft 365 email account use, students understand and agree that:

- the email account must be checked on a regular basis
- it is a violation to give other people access to your account or password; use by anyone not authorised by the College is prohibited and all attempts to access the service by authorised and non-authorised users may be logged
- it is expected that all important correspondence (both received and sent) will be kept
- any suspicious messages or attachments must be deleted without opening or downloading and reported to the IT Services at it@excelsia.edu.au; only open attachments from trusted source sites and always scan downloaded attachments for viruses
- all sessions must be closed by signing out on all public or shared devices.

In relation to harassment and spam, students understand:

- the Microsoft 365 email service shall not be used for any illegal purpose, must not be used to harass any organisation or individual (including sexual harassment), must not be used to access, duplicate or forward obscene, pornographic or indecent matter or material that may be considered to be obscene, pornographic or indecent by others, must not be used to duplicate or forward any email that pertains to contain information about potential computer viruses or email considered to be 'spam'
- the email service must not be used to send unsolicited commercial emails, and students are not authorised to send individual or group emails that announce, advertise or inform unconsenting users. All advertising of student events will be through the College Marketing Department.

In relation to privacy, students understand:

- emails in Microsoft 365 are stored on an external server and, although not viewed, emails in the inbox or any other folder cannot be considered confidential. Emails that are considered sensitive or confidential should be removed from the server as soon as possible. For more information about the College Privacy Policy, please refer to the Information Management and Privacy Framework and the Student Handbook.

8 Document status and governance

Responsible Officer	Chief Financial Officer	Date created: August 2023 Date of last review: August 2023
Approving Authority	Management Committee	Meeting date: 13 October 2023 Agenda item number: 8.3.2
Publication	Version 1 (Public)	October 2023
Related documents and references	**External documents** *Government Information (Public Access) Act 2009* (NSW) *Health Records and Information Privacy Act 2002 No 71* (NSW) Higher Education Standards Framework Threshold Standards (2021) *Higher Education Support Act 2003 (Cth)* *Privacy Act 1988 (Cth)* *Privacy and Personal Information Protection Act 1998 No 133* (NSW) **Internal documents** CO-STA-01 Staff Code of Conduct FIN-STA-01 Financial and Administration – Staff Framework	

	GOV-GS-STU-01 Code of Conduct for Students GOV-STA-04 Information Management and Privacy Framework PLA-GEN-07 ICT Plan 2020–2025 PLA-GOV-02 Operations Continuity Plans	
HESF	2.1, 3.3, 7.2, 7.3	
Review date	Review of Version 1	October 2026

9 Document history

This policy framework has been amended as follows:

Version	Approved by and date	Sections amended