Bring Your Own Device (BYOD) Agreement

Reviewed:	September 2024
Next Review:	September 2025

Vision

Loreto College is centred in God, rooted in Christ and animated by the spirit of Mary Ward, the founder of the Institute of the Blessed Virgin Mary. Our vision is that it will be an educational community where each person has the experience of being loved and valued as a sacred individual created by a loving God; a community where students enjoy an enriching and liberating education that helps them grow into the fullness of life and empowers them to be men and women of courage who are alive to the needs of humanity and committed to making a better world.

General Information

Users are expected to use personal ICT devices in accordance with the College's Online Safety, Information Security, GDPR policies and ICT User / BYOD agreements. This policy covers use of the college's systems both on college premises and remotely. It covers all devices to access college systems including but not limited to laptops, tablets, home desktops, and smartphones, and includes the use of college owned devices and personally owned devices.

Guidelines for acceptable use

Detail on what is acceptable is to be found in the staff and student ICT user agreements – all use must be responsible, professional and respectful.

Users may use their devices to access the following college resources:

- Email
- Intranet
- Remote desktop - staff only
- Virtual Private Network (VPN) – limited to selected staff
- Network access to selected drives
- Cloud based:
    - Microsoft Office 365
    - Course specific teaching and learning resources

There are restrictions in place on the use of certain social media platforms and applications using the college's internet access. All use of college owned devices must be in accordance with the law.

Security and online Safety

Loreto is aware that the breadth of issues classified within online safety is considerable, but can be categorised into four areas of risk:

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

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

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

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

Detail on security and online safety can be found in the college's Information Security and Online Safety policies.

- Users must not access inappropriate content on personal devices when using their own mobile data on college premises as outlined in the ICT User Agreement
- Users are responsible for their own property. The college is never responsible for the loss of or damage to the device or storage media on the device however caused.
- All staff personal devices used to access college systems must be enrolled via the college portal and only devices meeting the security compliance criteria will be able to access college systems
- Users need to be aware that any enrolled devices may be subject to checks as part of a security audit and verification process – these checks may involve installing an application and downloading files onto the device, or taking and sending screenshots of device settings but no personal data will be accessed and the user remains in control of the device
- All laptops and all devices used to access college systems must have up-to-date anti-virus software installed and operational
- The college takes no responsibility for the security, safety, theft, loss, insurance or ownership of any device brought onto the college premises which is not defined as the property of the college
- Devices must never be taken into controlled assessments and/or examinations, unless special circumstances apply
- Devices must be used in accordance with the relevant Staff or Student ICT User Agreement
- Users must take all sensible measures to protect information including but not limited to the use of authenticated access to their own device (i.e. requiring a PIN, pattern or password to be entered to unlock the device). Users should also ensure that the device auto locks if inactive for a period of time
- Users must ensure they have unique logons for their devices
- User should not allow shared access to their college account
- Users must check their personal ICT devices to ensure the devices are free from unsuitable material and free from viruses etc. before bringing the device into college
- The College takes any security incident involving a staff member's personal device very seriously and will always investigate a reported incident. Data protection incidents and the loss or theft of a personal mobile device should be reported to the Data Protection Officer
- The college reserves the right to remotely wipe any college data from a device
- Where possible all college documents should be edited using Microsoft Office on-line applications. Where not possible any downloads should be deleted once the file has been saved back to the college network
- Users must only use their college email address for the purposes of college related communications

Risks, Liabilities and Disclaimers

The college reserves the right to disconnect users' devices from the college network without notification.

Lost or stolen devices belonging to staff must be reported to the Data Protection Officer within 24 hours in order for college data to be wiped.