Our Requirements

Technology & Cybersecurity

Why is this important?

By standardising and following technology and cybersecurity requirements, we can protect our digital assets' confidentiality, integrity and availability from misuse, attack, damage, failure, loss or unauthorised access.

Document control
This document is uncontrolled when printed or downloaded and should be discarded after use. Always source the most recent version from the White Rose *Governance Fundamentals Library* and share only the document link.

Document title	**Technology & Cybersecurity**	Verbatim of above
Identification	**OR011**	A unique identification number: letters followed by three digits.
Status	**Published**	The lifecycle status: draft/published.
Version	**1**	Major number only (0=draft; 1; 2; etc)
Approval Date	**26 February 2026**	The date this version of the document was approved
Revalidation Date	**26 February 2028**	The date the document is due for review. A maximum of two years after the approval date.
Approver	**Lee Mason**	Title of the person who owns and is responsible for the document

Revision History		
Revised by	Revisions/changes/comments	Date re-published
Lee Mason	**First publishing**	

Table of Contents

1. Logon notice for our Information Technology (IT) system

Please see Appendix A for logon notice for our Information Technology (IT) environments.

2. Privacy notice

Please see Appendix B for privacy notice.

3. Your responsibilities

When requesting or introducing any technology:

- Engage the Technology functional representatives
- Do not purchase or enter into contracts for technology (including services) without approval (approved by White Rose technical leadership, or Client, whichever relevant)
- Do not use unauthorised technology hardware or software (approved by White Rose technical leadership, or Client, whichever relevant)

At all times:

- Use a long and strong passphrase
- Learn to detect phishing email and report/block via your email tool
- Only use White Rose approved applications (see Appendix C)
- Provide access to technology systems based on the principles of least privilege, and only for the duration of the business requirement
- When creating data or information, classify it in accordance *Our Requirements for Information Governance and Controlled Documents,* and protect it with the principles of least privilege
- When creating data or information that is considered a Privacy risk, such as Personal Information (PII = personal identifiable information) (see Appendix B for fuller definition), then password protect it and/or ensure that access is limited to those with a need-to-know
- Use multifactor authentication (MFA), including one-time passwords (OTP) for accounts with administrative privileges and for all remote access
- Use the company-provided VPN
- Perform user access reviews: Privileged accounts – quarterly; End-user accounts – quarterly.
- Make sure system backups meet or exceed the business continuity targets
- Ensure all hardware and software used has appropriate security protection, including patches and malware controls
- Consider audio-visual security to protect information from compromise by unauthorised persons
- Report any suspected security events to your 1-up and our DISP Security Officer
- Do not connect removable media (USB, hard drives, phones, etc.) to systems owned or managed by White Rose unless there is a valid business purpose.
    - If there is a valid business purpose, erase all White Rose data from the removable device when it is no longer required.

4. Cybersecurity Framework

The cybersecurity risk framework encompasses not only our documentation, our *Code of Conduct* and *Our Requirements* but also our processes and methods as they apply to personnel and physical security.

Scenarios

Some potential cybersecurity risk scenarios as they relate to White Rose:

- A malicious actor deliberately targets and takes control of the system
- White Rose is affected by a widespread cyber-attack targeting a specific industry, geography, or tool
- A third-party service is impacted by a cyber event resulting in loss of system

Causes

Some potential cybersecurity risk causes as they relate to White Rose:

- A user falls for a phishing email and deploys malware by clicking links or gives away passwords by entering details to a malicious site
- Compromise of privileged accounts results in authorised access to the system
- Technical vulnerabilities exist and are exploited to gain unauthorised access to the system
- Unauthorised physical access is obtained to locations that house system
- A third-party service is compromised, which enables unauthorised access to White Rose information they hold or to a White Rose system
- Ineffective backup and recovery systems

Controls

We leverage the ASD8 framework to strengthen and continuously improve our cybersecurity posture. At a minimum, White Rose will implement and maintain Maturity Level 1 for all eight controls. But our focus on continuous improvement will assure we build and attain additional Maturity Levels, commensurate with our assessed risk profile.

The ASD8 controls we measure against include:

- Application control
- Patch applications
- Configure Microsoft Office macro settings
- User application hardening
- Restrict administrative privileges
- Patch operating systems
- Multi-factor authentication
- Regular backups

Additional controls

White Rose implements additional controls, commensurate with our assessed risk profile. These include:

- Configuration baseline profiles applied (O365)
- Email phishing / spam controls (Microsoft EOP)
- Data encryption at rest (BitLocker)
- Data encryption in flight (VPN)
- Anti-virus (Microsoft Defender)
- Incident response (outreach to Supplier, Client and ACSC)
- Password protect Personal Information (PII = personal identifiable information), and/or ensure that access is limited to those with a need-to-know

Appendix A - White Rose Information Technology (IT) logon notice

This is a White Rose owned computer system and is the property of White Rose.

This system contains confidential, proprietary, and other information protected by administrative, civil, and/or criminal penalties against unauthorised users.

It is for authorised use only. Users (authorised or unauthorised) have no explicit or implicit expectation of privacy.

Any or all uses of this system and all files on this system may be intercepted, monitored, recorded, copied, audited, inspected, and disclosed to authorised administrators, White Rose, its representatives, and law enforcement personnel, as well as authorised officials or other agencies.

By using this system, the user consents to such interception, monitoring, recording, copying, auditing, inspection, and disclosure at the discretion of authorised administrators or White Rose company personnel.

Unauthorised or improper use of this system may result in administrative disciplinary action as well as civil and criminal penalties.

By using this system you indicate your awareness of an consent to these terms and conditions of use.

Do not use the White Rose system if you are not authorised to access or use it, or if you do not agree to the conditions stated in this warning.

Appendix B: Privacy Notice

Protecting your privacy is very important to us. For the purposes of this notice, **personal information** means any information about an identified or identifiable person. This includes where you can be identified, directly or indirectly, including by reference to an identifier (for example, a name or email address). We use words like **process** and **processing** to describe the various things we may do with your personal information – including using, disclosing, holding, recording, storing, transferring or otherwise handing that information.

Who does this notice apply?

Everyone who works for White Rose (**you**), and White Rose (**UBH**, **we**, or **us**).

Types of personal information we collect

We will primarily collect personal information from you either directly (such as when you work for us) or indirectly from your interaction with us (such as use of our IT systems).

The types of information we collect may include:

- Identification data – such as your name, gender, photo, and date of birth
- National identifiers – such as your passport details or security clearance information.
- Contact details – such as your home address, email address and mobile phone number. This may include contact details of your next of kin or emergency contacts.
- Recruitment records – such as your work application form, resume or CV, interview notes, references and any results of background checks
- Worker records – such has your position name, office location, employment contract, attendance records, health and safety records, performance records, skills records, training records, records of projects you have worked on, termination / resignation records.
- Financial information – such as banking information, tax information, salary, benefits, and payments records.
- IT information – this includes information required to provide access to our IT systems such as login information, IP addresses, and records of your use of those systems such as email.
- Other information – such as access and attendance to White Rose premises such as security records of times of entry/exit, and information collected through CCTV, and any other information you voluntarily provide to White Rose.

Why we process your personal information

The purposes for which we process your personal information will depend on the type collected and the context in which it is collected. However, the primary purposes for which we process personal information include:

- Managing your working relationship – recruitment, salary, performance.
- Managing our workforce – financial planning, managing our IT systems, building access and security.
- Managing our contractual relationships – managing and fulfilling contracts with customers, suppliers and third parties.
- Managing safety and security risks – building access and security, IT system access and security.
- Legal obligations – meeting obligations under contracts or law, responding to lawful requests.

With whom we share your personal information

Disclosures within White Rose

We may share your personal information within White Rose who require the information for the purposes of this notice ('why', above).

Disclosures outside White Rose

We may need to share your personal information with:

- People you have authorised to interact with us on your behalf (such as client)
- Third parties who provide services we use to run our business (IT, pay, etc)
- Our professional advisors (legal, accountants, etc)
- Government authorities or others obliged by law

How we store and protect your personal information

Information Security

We put in place procedures and technologies to maintain the security of your personal information from the point of collection to the point of destruction. For example, access to personal information is by "need to know" basis, and we aim to apply access control mechanisms to personal information.

Storing personal information

We generally store personal information within our electronic databases (IT system). We use third parties to store and process your personal information, however, we only do this when we determine the party complies with our procedures and policies, or if they put in place equivalent or better measures.

Information retention

Our aim is to keep personal information for no longer than is necessary for the purposes described in this notice. Please see *Our Requirements for Information Governance and Controlled Documents*.

Your rights and choices

If you wish to access, correct or update any personal information then please contact HR or your 1-up.

If you are concerned about how we are dealing with your personal information, then you may have the right to complain to an applicable data protection authority – in Australia, this is the *Office of the Australian Information Commissioner*. Before raising a complaint, we recommend that you first raise the issue with us so we can address your concerns as quickly as possible.

In addition to the above, you have the right (in certain circumstances) to request:

- The erasure of any personal information that we hold about you;
- The restriction of processing of any personal information that we hold about you; and
- The transfer of your personal information from White Rose to a third party.

Appendix C: Approved applications

White Rose uses all SAAS products.

Approved user applications are:

- 0365
- Microsoft Authenticator
- Adobe Pro
- NordVPN
- Corporate Traveller

Approved functional applications are:

- Xero
- Banking applications
- Monday CRM
- Approved government portals

Approved IT administrator application are:

- WIX
- Go Daddy