COLLABORATION AND CYBER SECURITY GUIDELINES	
Name	
Job Role/Title	Team Leader for Bounce Fitness
Workplace/Organisation	Bounce Fitness
State/Territory	

A. PROTOCOLS FOR COLLABORATIVE KNOWLEDGE SHARING

[Approximate word count: 150 – 200 words per protocol]

Assessor instructions: The student must include at least **two** protocols for sharing knowledge collaboratively in a virtual work environment.

These refer to guidelines and procedures on how individuals and teams will collaborate to share information, insights and expertise within a virtual or remote work setting.

Protocols for sharing knowledge collaboratively can include three or more of the following:

- Access and permissions for creating, editing and viewing documents
- Document versioning and control
- Use of appropriate channels for specific types of communication
- Process for real-time collaborative editing
- Process for providing feedback and resolving queries
- File naming convention
- Labelling documents with sensitive information
- Establishing knowledge database
- Data backup and recovery

The student must show that each protocol for sharing knowledge aligns with the team's work details.

The assessor must refer to the work details outlined in the **Team Protocol SOP Template**.

At a minimum, each protocol must:

- Directly relate to the tasks the team performs.
- Seamlessly fit into existing work processes without causing disruption.
- Can be customised to suit different types of work within the team.
- Can result in consistent and high-quality work output.
- Can contribute to increased efficiency in completing work tasks.

The student must show that each protocol for sharing knowledge aligns with the team's objectives.

The assessor must refer to the team objectives outlined in the **Team Protocol SOP**.

At a minimum, each protocol must:

- Explicitly support the achievement of team objectives.
  For example, the team objective is to improve cross-functional communication; the protocols include emphasising effective communication channels.
- Have measurable indicators to assess their impact on team objectives.
- Encourage collaboration among team members.
- Can adapt to evolving team objectives and changing project goals.
- Incorporate feedback mechanisms from team members.

a.
b.

B. PROTOCOLS FOR CYBER SECURITY

[Approximate word count: 150 – 200 words per protocol]

Assessor instructions: The student must include at least **three** cyber security protocols the team must follow in a virtual work environment.

These refer to guidelines and procedures on how individuals and teams will protect computer systems, networks and data from theft, damage or unauthorised access.

Cybersecurity protocols for virtual work environments can include three or more of the following:

- Use of multi-factor authentication (MFA) for company systems and accounts
- Use of secure virtual private network (VPN)
- Schedule for regular software patching and updates
- End-to-end encryption for all communication channels and sensitive data
- Setting user access controls
- Security awareness training
- Development and update of incident response plan
- Cyber security audits and assessments
- Secure cloud practices
- Device security guidelines
- Regular password updates

The student must show that each cyber security protocol for sharing knowledge aligns with the organisation's cyber security procedures.

At a minimum, each protocol must:

- Be consistent with the organisation's established cyber security guidelines and standards.
- Adhere to relevant cyber security regulations and compliance requirements applicable to the organisation's industry.

e.g. protection of individual's privacy in line with the Australian Privacy Principles (APP)

- Integrate with the organisation's risk management framework, addressing identified cyber security risks and threats.
- Be consistent with the organisation's training and awareness program.

E.g. regularly training on cyber security best practices

a.
b.
c.

END OF COLLABORATION AND CYBER SECURITY GUIDELINES TEMPLATE