National Protective Security Authority

National Cyber Security Centre

TOREN CONSULTING

SHARED WORKSPACES

Security Guidance for Users

INTRODUCTION

Shared workspaces offer flexible and cost-effective solutions for individuals and organisations. From coworking spaces and private offices to shared laboratories and manufacturing facilities, these environments are designed to support creativity, collaboration, and scalability. They cater to a wide range of users, including researchers, startups, and established businesses, offering advanced resources and fostering partnerships without long-term commitments.

However, shared workspaces also bring unique security challenges. Whether you're hot desking in a coworking area, running experiments in a shared lab, or using specialised manufacturing equipment, sensitive information, devices, or intellectual property can become vulnerable to unauthorised access or accidental exposure. Each type of workspace, from hot desks to confidential executive suites or R&D labs, presents different risks.

This guidance is for users of shared workspaces and provides practical advice tailored to your workspace and activities. The guide uses a risk-based approach to provide security considerations to help you safeguard your assets and key questions you should be asking your provider. By categorising spaces into open, private, and confidential environments, the guidance ensures you can identify the measures most relevant to your circumstances.

By understanding the risks and applying appropriate steps, you can fully embrace the benefits of shared workspaces while protecting what matters most.

Shared workspace providers will also benefit from reviewing the Trusted Research and Secure Innovation campaign information, published by NPSA and the NCSC.

Find out more:
Trusted Research
Secure Innovation

TYPES OF SHARED WORKSPACES

Shared workspaces come in many forms, supporting a diverse range of users and activities. From coworking spaces and private offices to shared labs and innovation hubs, these environments serve professionals, researchers, startups, and established teams.

The categories below illustrate the variety of shared workspaces, helping you recognise the type of space that best reflects your own working environment.

Coworking spaces

Flexible work environments with desks in an open area on a first-come, first-served basis (hot desking) supported by communal facilities like meeting rooms.

Shared Laboratories

Shared labs provide cost-effective access to specialised lab equipment for researchers and startups. They often promote community and collaboration.

Private offices in shared building

A private area within a coworking or other shared facility. Allows the users to manage their own space while still benefitting from shared resources.

Catapults

Innovation hubs connecting businesses, engineers and researchers to turn ideas into market-ready solutions. They often include shared workspaces along with other benefits.

University Spaces

University-based hubs foster partnerships between academia and industry, and support research and real-world applications of innovative ideas.

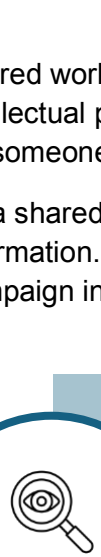
Incubators/Accelerators

Programmes for startups, offering mentorship, funding connections, and shared resources (including hot desking and private offices) to encourage growth.

WHO ARE YOU AT RISK FROM?

Shared workspaces can present relatively easy targets to people seeking unauthorised access to sensitive company information such as research or intellectual property. The same open, collaborative environments that make them popular with individuals and growing businesses mean that it can be easy for someone with ill intent to have, or appear to have, legitimate access.

As a shared workspace user, it is important that you understand the key threat actors that might seek to exploit these vulnerabilities to gain access to your information. For the latest threat information, please refer to the NPSA, NCSC and MI5 websites and the '*Secure Innovation*' and '*Trusted Research*' campaign information.



State Actors

Some foreign governments target UK businesses to steal technology and intellectual property, fast-tracking their own capabilities.

This can hurt your business by undermining your competitive advantage.

Competitors

Rival companies may try to gain access to your data or ideas to get ahead in the market.

They might have legitimate access to your shared facilities, allowing them to see written information or overhear meetings.

Cyber-criminals

Cybercriminals may target company systems for financial gain.

Tactics involving wireless networks, phishing or compromising unprotected devices may be easier to accomplish in a shared workspace setting.

Opportunistic Thieves

Many of the same security vulnerabilities in shared workspaces that could be exploited by more sophisticated threat actors are also exploited by casual thieves. The impact of loss of your IT assets and IP might be similar, regardless of the thief's motivation.

Activists

Groups with a specific agenda may target organisations, research companies or the shared workspaces providers hosting them or their events.

Activist activities may include protests, disruption or sabotage in both physical and cyber forms.

REMEMBER...

Any of these threat actors could present as legitimate shared workspace users, visitors, contractors, etc.

USER ARCHETYPES

Identify which archetype aligns most closely with your circumstances to find tailored guidance on managing security risks in your workspace. Turn to the next section for detailed guidance tailored to your workspace type.

While these archetypes illustrate some typical activities and security measures, they do not cover every individual situation. The following pages provide more in-depth guidance depending on the type of space that you're using.

	The Independent Researcher	The Growing Small Team	The Sensitive Project Team
Profile	Solo professionals, such as researchers or consultants, using hot desks for affordability.	Small teams needing flexible, private office space that can scale with their business.	Teams working on confidential projects, such as collaborative R&D.
Workspace Needs	Desk space and a fast internet connection for day-to-day tasks. Access to call booths for sensitive discussions and semi-private booths for screen work.	Private space for team collaboration and confidentiality. Access to communal resources like meeting rooms.	Private workspace with enhanced confidentiality measures. A workspace provider that is able to provide enhanced security measures.
Security Considerations	Selecting a workspace which provides access to appropriate semi-private spaces. Ensuring device and document protection in communal areas.	Maintaining flexibility of size of private space while maintaining control over access. Ensuring that shared resources outside of the private space are used appropriately.	Selecting a workspace and provider that can meet third-party security requirements. Considering other users of the workspace and their impact on security.
User Category Recommendation	Primarily **OPEN** and may need to move to **PRIVATE** if work is sufficiently sensitive.	**PRIVATE**, but mindful of **OPEN** guidance when using shared resources or open areas.	**PRIVATE** or **CONFIDENTIAL** depending on the project or client security requirements.

PROPORTIONATE SECURITY MEASURES

We understand that shared workspace users want to make the most of shared workspace benefits while managing security risks. Another key consideration is that shared workspace users will require the use of different spaces and functions at different times.

This guidance therefore categorises shared workspaces into three distinct groups (capturing different types of space from hot desks and shared equipment through to private spaces and dedicated confidential suites) and describes the security measures applicable to each category. These are: **OPEN**, **PRIVATE** and **CONFIDENTIAL**.

For example, a user with a **PRIVATE** office may want to use the **OPEN** hot desking area for a while; this guide helps them to understand how to do that appropriately. Alternatively, a user may want to upgrade to a higher security **CONFIDENTIAL** facility to meet client requirements, in which case this guide helps them to understand what they could ask their shared workspace to provide.

The measures recommended for **OPEN** workspaces focus primarily on awareness and decision-making, whereas those for **PRIVATE** and **CONFIDENTIAL** spaces extend to cover routine activities and options for security enhancements. Importantly, none of these categories imply that a user takes no action.

	OPEN	PRIVATE	CONFIDENTIAL
Description	Users share workspace and facilities, e.g. shared equipment in laboratory and manufacturing spaces or coworking desks. There is limited control over physical access to individual work areas. Security considerations focus on general security awareness, maintaining confidentiality and safeguarding portable assets in open areas.	Users have exclusive use of an enclosed workspace, such as private offices and individual laboratory spaces. Users have control over access and some ability to install their own equipment. Security guidance seeks to maximise the benefits of ownership and control in the context of a wider shared workspace.	Users routinely handle sensitive information in workspaces that, while shared, were designed with security in mind. Users benefit from the workspace provider's enhanced security measures. Security advice attempts to anticipate sensitive client requirements and advise on how to select an appropriate provider.
Examples	• Hot desks • Assigned desks in open areas • Communal lab benches • Shared equipment	• Private offices • Dedicated project rooms • Dedicated laboratory and manufacturing spaces	• Confidential project rooms • Sensitive lab or R&D suites • Secure executive suites

Note: Users of principally 'Confidential' workspaces should still consider the applicability of guidance for 'Open' and 'Private' workspaces. This is because workspaces catering for users with sensitive information often also include an element of open and enclosed workspaces for supplementary or occasional use.

SECURITY CULTURE

Developing a security culture is a journey that evolves with your workspace and needs. Whether working in open, private, or confidential spaces, start with basic awareness and build towards stronger practices. Use this guidance to embed good security behaviours, protect what matters most, and make security a shared responsibility.

Workspace	Focus	Building Security Culture
 **Open Workspaces**	Awareness and shared responsibility	**Awareness First**: Understand the risks of shared spaces, such as tailgating or overheard conversations. **Normalise Reporting**: Create a culture where reporting suspicious behaviour or misplaced passes is second nature. **Take Responsibility**: Adopt and comply with good security habits, like securing devices and documents when you are not using them.
 **Private Offices**	Control and team accountability	**Set the Example**: Exemplify and promote security-conscious behaviours within your team. **Monitor Access**: Ensure everyone takes ownership of monitoring access into your private workspace. **Collaborate with Providers**: Work closely with your workspace provider to address potential vulnerabilities in both common areas and your private space.
 **Confidential Spaces**	Compliance and regular review	**Maintain Sensitivity Requirements**: Reinforce careful handling of sensitive material through regular discussions and training. **Set Expectations**: Establish clear expectations with workspace providers to meet stringent security needs. **Refine Regularly**: Periodically review incidents and adjust security behaviours to stay aligned with best practices.

PRIVACY IN THE WORKSPACE

As some of the key benefits of shared workspaces are collaboration and networking, it is to be expected that ensuring privacy may be a challenge. Nonetheless, it is possible to choose a shared workspace that allows you to manage your privacy as well as possible, and to act in way that makes it more difficult for someone to overhear or view your sensitive information.

	OPEN	PRIVATE	CONFIDENTIAL
 ***Selection Criteria***	Choose a workspace with bookable meeting rooms and individual call booths. Use providers with a straightforward system for reporting suspicious behaviour or security concerns.	Look for workspace providers who will allow you to fit simple privacy measures to your space.	Discuss your third-party security requirements with your provider before signing a contract.
 ***Physical Enhancements***	Install privacy screens on laptops. Use lockable cabinets and storage facilities for your personal items.	Install blinds or privacy film to glazed partitions and windows[1]. Install secure cabinets for sensitive hardcopy information. Provide your office with a shredder or arrange a confidential waste disposal service.	Consider installing tamper-resistant[2] locks to offices and storage containers.
 ***Behaviours***	Select a desk away from high traffic areas. Take documents and devices with you when stepping away, even briefly. Be aware of your surroundings when handling sensitive information. Use call booths or meeting rooms for sensitive discussions. Clear data off shared equipment after use.	Use a protective marking scheme and maintain a register of sensitive documents. Store sensitive documents in a secure container when not in use. Lock electronic devices in secure storage overnight or take them home with you.	Escort third-party staff such as cleaners and contractors when they need to enter your space. Instruct your provider not to publicise your use of the building, e.g. by excluding you from publicity and displayed tenant lists. Periodically review any agreements with workspace providers to ensure your privacy preferences (e.g., excluded from tenant lists) are being respected.
 ***Governance***	Outline shared responsibilities for security in provider agreements, such as users keeping desks clear and providers managing access.	Check your workspace provider's vetting policy for people who need access to private offices, e.g. cleaning and maintenance.	Ensure your provider has a robust third-party audit process to monitor compliance with their promised standards.

Note: Users of principally 'Confidential' workspaces should still consider the applicability of guidance for 'Open' and 'Private' workspaces. This is because workspaces catering for users with sensitive information often also include an element of open and enclosed workspaces for supplementary or occasional use.

ACCESS MANAGEMENT

Some shared workspaces are deliberately relaxed about entry, while others are poorly designed with regard to overseeing and managing their entrance routes. It's important that you choose a workspace that manages access well. The NPSA website has detailed advice on access control measures.

	OPEN	PRIVATE	CONFIDENTIAL
Selection Criteria	Ideally, choose a workspace which uses speed gates to control access. As a minimum look for a well-located, permanently staffed reception desk supervising entry.	Choose a workspace that provides encrypted electronic access control to your private space, rather than a lock and key. Choose a workspace that uses an electronic visitor management system.	Choose a workspace with robust electronic access control that is aligned to your requirements. This may mean, for example, multifactor authentication and / or access portals rather than turnstiles.
Physical Enhancements	*Access control in flexible / private spaces is installed and managed by the workspace provider. Ensure you review the current arrangements to check if they meet your requirements.*		Consider implementing enhanced access control credentials (e.g. multifactor authentication or biometrics) to your private space[3].
Behaviours	Be aware of tailgating and report any incidents to the provider. Report any issues with the access control system to the provider.	Ensure that the door to your private space is closed and locked each time you leave. Instruct your team to use their assigned access credentials individually (no sharing) to maintain access integrity. Instruct your provider to remove access when an employee or contractor stops working for your organisation or team.	Regularly review access control logs for your workspace areas.
Governance	Confirm that the provider has a process for: • booking in visitors and verifying their identity. • removing access for people who no longer use the space. • investigating unauthorised access incidents and communicating resolutions.	Ensure that your provider has a process for managing access to private spaces for cleaners and contractors. This should include checks to avoid sharing of access credentials between workers.	Instruct your provider to give you regular reports from their access control and visitor management systems. Ensure your provider has a robust third-party audit process to monitor compliance with their promised standards.

Note: Users of principally 'Confidential' workspaces should still consider the applicability of guidance for 'Open' and 'Private' workspaces. This is because workspaces catering for users with sensitive information often also include an element of open and enclosed workspaces for supplementary or occasional use.

PHYSICAL SECURITY SYSTEMS

The extent of electronic security provided to shared workspaces varies significantly. While many have access control (see above), this may be more to monetise shared resources like meeting rooms rather than for security. Most providers deploy video surveillance at entrances and some in common areas. As many shared workspaces are accessible 24/7, intruder alarms are less common.

	OPEN	PRIVATE	CONFIDENTIAL
Selection Criteria	Ensure your provider has installed a video surveillance system with cameras viewing entrances and common areas.	Choose a provider who will allow you to install your own electronic security measures in your space.	Choose a provider whose installation and operation of security systems is aligned to your own and any third-party security requirements.
Physical Enhancements	*Security systems in common areas will be the responsibility of your provider.*	Consider installing your own intruder detection and video surveillance systems inside your private space[3]. Use systems that allow you to receive alarms and review video images remotely so that you can verify incidents when you're not there.	Install additional security systems and devices to your private area, to suit your own or any third-party security requirements[3]. Consider layered security measures, such as combining door monitoring and motion sensors for critical areas.
Behaviours	Select a desk where you and your belongings, but not your screen, appear to be overlooked by a surveillance camera. Report any damaged security devices to your provider.		Train staff to recognise signs of tampering or system failures and report them immediately.
Governance	Understand how your provider deals with, and responds promptly to, security incidents or equipment malfunctions. Confirm that surveillance footage is securely stored and accessible only to authorised personnel.		Ensure your provider has a robust third-party audit process to monitor compliance with their promised standards.

Note: Users of principally 'Confidential' workspaces should still consider the applicability of guidance for 'Open' and 'Private' workspaces. This is because workspaces catering for users with sensitive information often also include an element of open and enclosed workspaces for supplementary or occasional use.

CYBER SECURITY

The security of digital systems and information requires everyone to play their part. Cyber-attacks come in many shapes and sizes but the vast majority can be prevented by implementing a few basic actions. The National Cyber Security Centre (NCSC) has developed a range of guidance to support organisations and individuals protect themselves and to minimise the impact should an attack be successful.

Cyber Essentials (CE) is the UK Government's baseline standard for cybersecurity for organisations of all sizes. It is designed to help protect against the most common cyber-attacks by implementing five key controls (Firewalls, Secure Configuration, Security update management, User access control and Malware protection). Cyber Essentials is assessed by an independently verified self-assessment whereas Cyber Essentials Plus (CE+) includes a technical audit to verify that the controls are in place. The Cyber Essentials readiness tool provides a series of questions to help organisations prepare for CE. The NCSC's Cyber Advisor scheme offers cost effective security advice and support that focuses on implementing CE.

For individuals, the NCSC has advice that all users should follow to stay secure online under Top tips for staying secure online. If your requirements are particularly complex, consider the NCSC's Assured Cyber Security Consultancy Scheme for advice.

	OPEN	PRIVATE	CONFIDENTIAL
Selection Criteria	Choose a provider who offers secure Wi-Fi. W-Fi should be protected with a strong password, ideally with separate networks for visitors and workspace users.	Choose a provider who has a relevant cyber security accreditation, such as CE, CE+ or ISO 27001 (the international standard for information security management). Verify your provider's IT team has a procedure for addressing cyber incidents, such as data breaches or network intrusions.	Choose a provider that is willing to work with you to understand and manage cyber security risks, using a recognised standard framework.
Technical Controls	Implement the five Cyber Essentials controls and achieve Cyber Essentials or Cyber Essentials+ certification.		Conduct cyber security risk management, using the NCSC's Cyber security risk management framework, or ISO 27001. Use the risk framework to identify, assess and manage risks. Consider using tools to standardise the implementation of necessary controls. For example, using mobile device management software to configure mobile devices to a standard configuration from a central point.

Note: Users of principally 'Confidential' workspaces should still consider the applicability of guidance for 'Open' and 'Private' workspaces. This is because workspaces catering for users with sensitive information often also include an element of open and enclosed workspaces for more general use.

References

IN-TEXT REFERENCES

1: National Protective Security Authority (NPSA), *Windows & Glazed Facades* (https://www.npsa.gov.uk/windows-glazed-facades)

2: National Protective Security Authority (NPSA), *Tamper Indication* (https://www.npsa.gov.uk/tamper-indication-0)

3: National Protective Security Authority (NPSA), *Video Surveillance, Access Control, Detection & Control Rooms,* (https://www.npsa.gov.uk/video-surveillance-access-control-detection-control-rooms)

ADDITIONAL RESOURCES

National Cyber Security Centre (NCSC), *Cyber Essentials and Cyber Essentials Plus* (https://www.ncsc.gov.uk/cyberessentials/overview)

IASME and National Cyber Security Centre (NCSC), *Get ready for Cyber Essentials* (https://getreadyforcyberessentials.iasme.co.uk)

National Cyber Security Centre (NCSC), *Reports & advisories* (Reports & advisories - NCSC.GOV.UK)

Security Service MI5, *Threats and Advice* (https://www.mi5.gov.uk/threats-and-advice)

National Protective Security Authority (NPSA), *Threat Information* (https://www.npsa.gov.uk/threat-information)

National Protective Security Authority (NPSA), *Secure Innovation* (https://www.npsa.gov.uk/secure-innovation)

National Protective Security Authority (NPSA), *Trusted Research* (https://www.npsa.gov.uk/trusted-research)

National Protective Security Authority (NPSA), *Security Culture,* (https://www.npsa.gov.uk/security-culture)

Icons obtained through: https://storyset.com/

Images obtained through: unsplash.com, freepik.com, pixabay.com

TOREN
CONSULTING

This document has been prepared by Toren Consulting in partnership with NPSA and the NCSC.

Toren Consulting was founded on the belief that protecting our people and our belongings is one of the fundamental reasons that humans build.

As built environment security design specialists, we aim to be respected professionals and valued members of property design teams. We emphasise a people-first approach, prioritising user experience and collaboration with stakeholders to deliver practical, buildable security solutions.