# Summary of responsibilities for all staff

This document summarises the content of the **Technology and communication services governance policy** that relates to users of our systems. For the fullest understanding, the main policy document must be read.

| | |
|---|---|
| Security | • Access to data, even if held on paper, must be restricted to those who need this access.<br>• Don't copy data belonging to Key to removable, storage such as USB drives.<br>• Everyone gets the minimum access to network services, software and data needed to do their regular, daily tasks.<br>• Exercise good judgement when using the web.<br>• You must not view non-work-related web content.<br>• Keep your password confidential and do not share it.<br>• All work accounts must have multi-factor authentication enabled.<br>• Only equipment provided by Key can be connected to wired or corporate Wi-Fi networks.<br>• Use public Wi-Fi networks only for accessing virtual desktop services. |
| Devices and services | • Lock your devices when unattended.<br>• Don't store device passwords or PINs where others can access them.<br>• ICT ensures applications and third-party services are securely configured and managed.<br>• If we provide you with a device, you must bring it and its charger to work.<br>• Connect work devices to Wi-Fi in Key's office and when at home.<br>• Report damaged or lost devices to ICT immediately.<br>• Use only Microsoft 365 apps for messaging and collaboration.<br>• Use Key email services only for business purposes.<br>• Anything sent or received on Key devices/services is not private. |
| Procurement | • ICT handle all technology and communication purchases.<br>• Pay-as-you-go mobiles are not allowed. |
| Data protection | • You cannot keep personal data for longer than it's needed.<br>• Individuals can request data erasure when it's no longer needed.<br>• Key must be able to justify how long personal data is kept.<br>• You must not print outside of Key offices and worker bases. |
| Data handling and retention | • Store files in the appropriate folders within Microsoft 365 and VDI.<br>• Don't copy files to personal devices or cloud storage.<br>• Data retention periods are detailed in the data retention policy. |
| Bring your own device (BYOD) | • Use personal devices only when there is no other alternative.<br>• Protect personal smartphones or tablets with a 6-digit PIN and regular security updates.<br>• Use Microsoft 365 mobile apps for work and remove accounts when you leave us.<br>• Use personal computers only for virtual desktop service.<br>• Personal computers must have an account used only by you and an active anti-virus/malware subscription.<br>• Don't connect personal devices to wired or Wi-Fi networks in the homes of people we support.<br>• Don't connect personal devices to office networks by cable. |

This summary relates to the **Technology and communication services governance policy** as published in May 2025.