Summary of responsibilities for all staff

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. • Don't copy data belonging to Key to removable storage devices. • Personal storage devices must never be connected to Key's equipment. • Everyone gets appropriate access to network services, software and data needed to do their regular, daily tasks. • Exercise good judgement when using the internet. • You must not view non-work-related internet content. • Keep your password confidential and do not share it. • All work accounts must have multi-factor authentication enabled. • Only equipment provided by Key can be connected to wired or corporate Wi-Fi networks. • Use Key's public Wi-Fi networks only for accessing virtual desktop services.
Devices and services	• Lock your devices when unattended. • Don't store device passwords or PINs where others can access them. • Key ensures that applications and third-party services are securely configured and managed. • If we provide you with a device, you must use it and bring it and its charger to work each day. • Connect work devices to Wi-Fi in Key offices and when at home. • Report damaged or lost devices to ICT immediately. • Use only Microsoft 365 apps for messaging and collaboration. • Use Key email services only for business purposes. • Anything sent or received on Key devices/services is not private.
Procurement	• Only ICT staff are authorised to make all technology and communication purchases. • Pay-as-you-go mobiles cannot be purchased by Key.
Data protection	• You cannot keep personal data for longer than it's needed. • Individuals can request Key to erase personal data when it's no longer needed. • Key must be able to justify how long personal data is kept. • Printing is only allowed within Key's premises.

Summary of responsibilities for all staff

For the fullest understanding, the main policy document must be read.

Data handling and retention	• Store files in the appropriate folders within Microsoft 365 and VDI. • Don’t copy files to personal devices or cloud storage. • 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. • Protect personal smartphones or tablets with a 6-digit PIN and regular security updates. • Use Microsoft 365 mobile apps for work and remove accounts when you leave us. • Use personal computers only for the virtual desktop service. • Personal computers must have an account used only by you and have an active anti-virus/malware subscription. • Don’t connect personal devices to wired or Wi-Fi networks in the homes of people we support. • Don’t connect personal devices to office networks by cable.