KANTAR

Cyber Security for Users

7 MINUTE READ

Our policy on...
Cyber Security for Users

First issued: March 2022

Last updated: June 2024

For all Kantar people

As a leading data and insights business, Kantar collects, processes and manages vast amounts of data, a significant portion of which is classified as personal information or personally identifiable information.

This work is enabled by the deployment of technology that empowers our users to connect to more data and applications, and provide our customers with more timely and accurate insights. It also gives us far more freedom about where, when and how we work. However, the use of technology also brings with it a different kind of risk and threat.

This short policy outlines the essential "Do's and Don't's" when working with Kantar systems, equipment, connectivity and data. By following these guidelines you'll be doing your bit to protect Kantar from cyber threats and all the financial, operational and reputational risks they represent.

This policy applies to all Kantar colleagues, permanent or contract, our suppliers and visitors to Kantar sites.

It covers the access and usage of Kantar Information Systems via Kantar supplied devices or use of an approved mobile device. It also covers the use of third-party Information systems, both when accessed from Kantar networks, and when accessed from personal networks (for example home networks or guest networks), for the purposes of fulfilling Kantar staff or contractor responsibilities.

Any breach of this policy may result in disciplinary action being taken including, in serious cases, potential dismissal or termination of a contingent worker's engagement. This policy is not part of your employment contract or contract for services and Kantar can change or update it from time to time.

01 Limiting personal use

Kantar allows for reasonable personal use of Kantar provided IT equipment and connectivity. Within that definition, please:

- Be aware of the personal information you communicate. Emails and messages are legal documents that may require disclosure under law, and submission as evidence in legal proceedings
- Don't forward or redirect any Kantar business information to any personal email account
- Don't knowingly access or search websites, or share links or material which include, but are not limited to material that is: Pornographic, sexually explicit, related to violence, hatred, illicit drugs, gambling, and/or any other inappropriate matter which causes or could intend to defame, harass, insult, offend, discriminate against, or intimidate another person or group of people
- Don't use Kantar systems, equipment or connectivity to run your own business.

02
Protecting Kantar Information Systems

Kantar may have provided you with a mobile device such as a laptop, tablet, or mobile phone or a combination of these to enable your work. Please:

- Do ensure your device is physically secure at all times, especially when working outside of Kantar locations
- Do disable all services like Bluetooth and Wi-Fi that you don't use to avoid connecting to public or unknown wireless networks accidentally
- Do ensure that your Kantar devices and documents are kept secure when not in use, unattended or when taken outside of a Kantar location or used in a public location
- Do Use 'Win+L' or 'Ctrl+Alt+Delete' then select 'lock' to lock your system before stepping away from your device
- Do action patch install notifications as soon as possible, and within specified timelines. Remember you sometimes need to re-start your device for the patch to be effective
- Do remember only Kantar managed or authorised devices are permitted to connect to the Kantar resources and network through either a wired or wireless connection. Authorised devices are typically those belonging to third parties such as contractors or consultants working for Kantar on Kantar premises, and the device access arrangements as stipulated in the relevant contract. Personal and guest devices, such as colleagues' personal mobiles and tablets, may connect to 'Guest Wi-Fi' if available
- Don't store any confidential or personal information in local drive of your system
- Don't connect any external storage device (such as an USB thumb drive, mobile phone or SD card) to any Kantar workstation, laptop, or mobile device
- Don't interfere, shutdown, bypass or modify any security applications or configurations on the device, or install (or attempt to install), remove or modify any security applications on the device
- Don't use any device for any unauthorised or inappropriate use such as hacking, introducing malware, or interfere or affect in any way with the normal operation or performance of the device, or any connected systems.

03 Using Kantar Information Systems Safely

Please:

- Do remember that publicly available instant messaging (such as WhatsApp, Facebook Messenger, iMessage) are not wholly appropriate for business (other than for approved use for research purposes) due to operational, legal and security reasons. Their use should be avoided for business-related communications. When the use of public instant messaging services is deemed essential (for example in an emergency), you are responsible for your use of that service and should keep such usage to a minimum
- Do comply with the requirements of the individual system you are using, and avoid having the same password for multiple systems or using the same password you use for personal e-mail and online accounts
- Do activate and use multi-factor authentication where it is provided
- Do always protect your account passwords, ensure you keep any physical or software tokens secured
- Do immediately report to the **Kantar Service Desk** if you believe your password has been compromised and/or authentication token has been lost or stolen
- Do ensure you visit only known, trusted and secure web sites (Check for https://, padlock symbols, privacy policies)
- Do contact Kantar via the **Kantar Service Desk** or email **soc@kantar.com** immediately if you feel your system is compromised or if it malfunctions as a result of your Internet or email activity
- Do report to the IT Service Desk when installed software or IT system access is no longer required for your role
- Do report any suspicious emails using the "**Report Phishing**" button in your outlook or email **phishing@kantar.com**. Be extra vigilant of attachments that come from an unknown source and don't forward to any accounts with the exception of **phishing@kantar.com**
- Don't share usernames or passwords
- Don't use any allocated privileged (Admin) accounts for regular user activities or for any purposes other than what it was provided for
- Don't download and install unapproved software or applications
- Don't download, copy, or transmit third party owned material without the consent of the license holder
- Don't knowingly send spam, unnecessary broadcast messages or chain messages in any format.

04 Processing Kantar Data securely

The data you process (which includes storage or transfer) during your work at Kantar is valuable, and must be kept secure and protected against unauthorised access. It's your responsibility to safeguard the Kantar data you are working on. Please:

- Do use Kantar's Microsoft Office365 subscription for storing and sharing Kantar data in line with Kantar's Data Handling Guidance
- Do ensure that your home network is secure. If you are using a home Wi-Fi connection, it must be securely configured (for example enabling WPA protocol and changing the default admin password) to prevent unauthorised access
- Do minimise the printing and storage of Kantar documents at home, and ensure they are securely disposed of using a home shredder. Alternatively dispose of the documents securely next time you are in a Kantar office
- Do ensure that your screen and any printed documents are not visible to others when being used in public locations
- Do avoid any conversations over telephone or video conferencing solutions where they may be overheard when discussing sensitive Kantar matters
- Don't use Public Cloud Services for the storage, processing, or sharing of Kantar Data unless they have been checked for compliance against Kantar Security policies and approved for use by Kantar
- Don't disable any Kantar provisioned security solutions on your device.

05 Key contacts:

If you would prefer to raise an issue of cyber security anonymously, you can use our **Right to Speak service**.

If you have any questions about this policy, please contact Alison Gallagher, Global Head of Compliance at **businessintegrity@kantar.com**.

Thank you for doing your bit to protect Kantar from cyber threats.