Information Systems Policy:

Acceptable Use of Information Technology

Current Release: February 25, 2015

Current Approval Date: February 25, 2015

Purpose: Define the acceptable and prohibited uses of information technology.

Scope: Applies to all Kantar operating companies, Kantar vendors who connect to Kantar networks or process, store, or transmit data for Kantar companies, and Kantar headquarters, regardless of legal entity status.

Editors: Kantar ITP Transformation Director and the Kantar CIO

Policy Owner(s): Kantar CIO and Kantar CFO

1. Policy:

As Kantar companies collect and process confidential client data, Kantar companies must conform to the Kantar Privacy Policy which can be found on https://insidekantar.com.

This Acceptable Use Policy reflects and upholds WPP policy regarding the use of information systems. All WPP policies can be found on http://inside.wpp.com.

EMAIL and MESSAGING

Access to the Internet and to digital messaging systems (e-mail, instant messaging, and other Company electronic messaging systems) will be made available to users at the discretion of the management of your Kantar Company. As with all Company information and communication facilities, Internet access and e-mail must be used responsibly. They are provided primarily for business purposes and not for personal use, although reasonable personal use will normally be granted at the discretion of your Kantar Company management.

Your Kantar Company and the Kantar ITP reserves the right to monitor and report on Internet, e-mail and instant messaging usage, including specific web sites accessed by individuals (where not prohibited by local laws).

Remember that digital messaging systems have the same legal standing as any other written communication and may be used as evidence in courts of law.

Business should not be conducted using personal e-mail accounts. Your Company must have access to all correspondence regarding its business, which may not be possible if personal e-mail accounts are used.

Email Forwarding: Automated processes to forward corporate emails to non-WPP email accounts or domains must not be used.

INTERNET USE

Internet access must not be used to download any programs, executable code, application add-ins or accessories, games or screen savers except where such downloading is inherent to a job role.

The Internet must not be used to access, view, download, post, or upload (and e-mail must not be used to distribute) any hate speech, racist, sexist, sexual, illegal material, material that may harass, or material which is likely to cause offence or to defame, misrepresent, damage, or bring into disrepute Kantar companies, its employees or management.

Recommendations on LinkedIn and Similar Sites: LinkedIn has a facility to allow subscribers to post “recommendations” for colleagues, ex-colleagues and other contacts. Where an individual makes this type of recommendation, making this posting can have a similar legal effect as that individual’s employer giving a written reference for all to see and rely on. This exposes the employer to unnecessary risks and so should be avoided.

This policy only applies to individuals “recommending” a fellow employee or external contact related to their employment – not to purely personal contacts.

Public File-Sharing Systems: There are a variety of publicly available, and often free, facilities to transfer large files without using email and to store data "in the cloud". These facilities must not be used for the transmission or storage of company and/or client data.

Kantar has established solutions for secure file transfer. Contact your IT service desk for further information.

SECURITY – COMPUTERS

All Company computing and messaging work must be done on Company-owned assets. However, your Company may provide network access for devices not owned by the Company via Outlook Web Access, Citrix, and other means. In such cases, Company data must not be written to devices not owned by the Company.

You must not disable or alter the configuration of anti-virus, wireless networking protection and other security software installed on any Company-owned computer.

Use of Personal Equipment: In no case are employees allowed to use personal computers in the office to carry out their work. Freelancers may use personal equipment with proper authorisation and security checks in place.

From time to time employees and freelancers may bring personally-owned storage devices (USB sticks, personal hard drives, etc) into the office. Such devices must not be used as routine storage for company information and, in the event that company information has ever been stored on these personal devices then Operating Companies should make clear to those bringing them in that the Operating Company reserves the right to inspect that equipment at any time to ensure that any company-owned and/or client data has been removed.

Non-Employees: People working at Company premises who are not employees must not use computers that are not owned (or leased) and managed by a Kantar Company or by a third-party under contract to provide IT services to a Kantar Company.
Where visitors (who are not employed by a Kantar Company) to Company premises are provided with Internet access or other computer facilities, this must be provided in a way that prevents them from connecting their computers to the Company network.

SECURITY - MOBILE and PORTABLE

Any laptop, smartphone, or portable device that receives Company messaging or data that is lost, stolen or compromised must be reported to the issuing department immediately.

Please ask your CIO for the Kantar Mobile Device Policy for further details on smartphone and tablet usage.

Kantar vendors who receive on their own mobile or portable devices Kantar confidential data or messages regarding the work they are executing for a Kantar company must encrypt that data and report any loss of such data to Kantar.

SECURITY - PASSWORDS

You will find that all access to Company networks is password-protected per WPP policy and that passwords must be changed every 60 days. WPP also mandates password-protected screensavers on all Company computers, with a maximum "wait" time of 30 minutes.

SECURITY - NETWORK CONNECTIONS

Connecting dial-up modems to workstations on the Company network is prohibited.
No wireless network access points such as wireless routers are permitted on Company premises without approval by the IT department.

SECURITY - OFFICE PREMISES

- Building access must be controlled such that all visitors who are granted access to the building are recorded in a log and are issued visitor badges.
- Identification badges and physical access cards that have been or are suspected of being lost or stolen shall be reported immediately.
- Report to your supervisor any person on Company premises whom you do not believe is authorized to be there.
- Access to information processing facilities and systems is granted only where there is a legitimate business need. Employees may gain access to and use only those systems for which they are specifically authorized.

COMPANY INTERNET SITES

Registration of all company web sites must be done through your Company IT Department or the Kantar ITP.

TECHNOLOGY DEVELOPED FOR CLIENTS

The intellectual property rights in any software developed for client use by your Kantar Company and provided as a service or product to a client must be protected.
Appropriate, legally binding terms and conditions must accompany all software provided

to clients such that the Company's risks are mitigated.

The provision of any IT hardware, software or services to clients must be covered by a written agreement, which has been reviewed by Company-appointed legal counsel and signed by both parties. Risks covered by such an agreement would include, but not be limited to:

- Maintenance of internal intellectual property and other copyright issues;
- Fitness for purpose (operating companies must avoid giving warranties);
- Support and maintenance procedures

BUYING COMPUTERS OR SOFTWARE

All software and hardware for Kantar employees must be ordered through your Kantar Company IT department according to WPP- and Kantar-mandated purchasing and licensing policies.

Only Company-owned or approved software may be installed on Company computers.

NEW BUSINESS SYSTEMS

No new business systems must be developed, purchased or implemented without approval from the WPP CIO and Kantar CIO. For this purpose "business systems" includes accounting, production, and timesheet systems.

DATA MANAGEMENT

All Company data must be stored on Company servers for backup and safe storage. Laptop and desktop users will be responsible for the security of data stored on those computers. All reasonable precautions should be taken to avoid loss, deletion or disclosure of such locally-stored Company data to unauthorised persons.

When not in use, confidential information, regardless of what media it is written to, must be securely stored to prevent unauthorized access, theft, or loss.

Company data must not be sent by any means outside the Company except where required to conduct your Kantar Company's business. Systems hosted outside the Company such as blogs, social networking sites, hosted collaboration tools and other companies' messaging systems are considered to be outside the Company.

Company confidential data must not be stored on removable media such as flash drives (thumb drives, memory sticks) unless encrypted using means authorized by your Company IT department.

All data and information created, stored, acquired or transmitted on Company computing systems must be exclusively owned by your Kantar Company (or client, in certain circumstances).

You must immediately report to your Kantar Company IT department any loss of data or if you suspect that an unauthorized party has attempted to access Company data or compromise Company security systems.

Any files, whether your own personal files or Company files, stored on Kantar Company computer or communication systems, will be treated as Company property and can be viewed by managers or other authorized personnel (where not prohibited by local law).

COPYRIGHT PROTECTION

Downloading, copying, possessing and distributing material (including documents, software, web page images, videos or text) via the Internet that infringes on copyright, trade mark rights or other intellectual property rights is prohibited.

2. Responsibilities and Roles:

You are responsible to uphold this policy and report any violation of this policy to your supervisor, your IT department, or, if a vendor, to your Kantar contact.

Kantar Companies IT departments are responsible to respond to reported violations of this policy and to such incidents as lost equipment or data to ensure Company information systems are properly secured and that required investigation of such incidents is executed. They are also responsible for providing information systems configured to be compliant with WPP and Kantar standards that provide security measures in this policy.

Kantar Companies management is responsible to promote compliance with and awareness of this policy among their staff.

3. Compliance:

Kantar employees may be disciplined in accordance with your Kantar Company's disciplinary procedures for breaches of any portion of this policy. Kantar companies' vendors may jeopardize their business with Kantar for any violations of this policy.

4. Exceptions:

Any exceptions to this policy must first be approved by the Kantar CIO or his designate and filed with the Director of IT Compliance and Governance.

5. Glossary

"your Kantar Company" - The Kantar Company that employs you or has contracted with you for Company work as a non-employee. All Kantar companies and Kantar, the holding Company, are included regardless of their legal status as a taxable entity.

Company - Refers either to "your Kantar Company" or any Kantar Company, depending on context.

Confidential Information - Data about all aspects of Company business and its clients, suppliers, and employees, not presently released to the general public.

Tablet – A wireless, portable personal computer with a touch screen interface. The tablet form factor is typically smaller than a notebook computer but larger than a smart phone.

Smartphone - Mobile phones with functionality to receive email and text messages as well as serving as a PDA.

IT - Information Technology

Kantar ITP – The Information Technology Partnership, the shared service for Kantar's information technology function serving a large segment of Kantar operating companies.

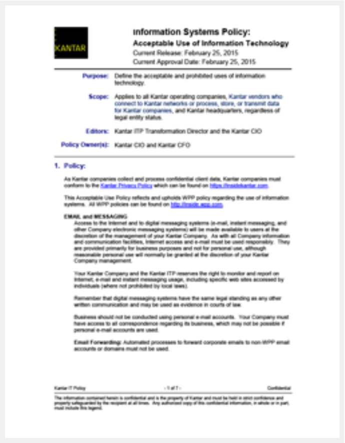
6. Revisions Table

Revisions	Editor	Approved By	Date
Created plus initial edits	Ron Thompson		January 15, 2010
Revised to serve as the only AUP to be used in Kantar	Ron Thompson	Matt Graham-Hyde	March 3, 2010
Added statement re: conducting business on personal email accounts and added the clause "except where such downloading is inherent to a job role" regarding downloading executables, etc.	Ron Thompson	Matt Graham-Hyde	May 25, 2010
Revised the "Security – Portable Computers, PDAs, Smartphones" section to no longer refers to Blackberry specifically but for users to check with their IT departments for current Kantar standards.	Ron Thompson	Matt Graham-Hyde	June 21, 2010
Revisions to several sections to reflect clauses in the 2011 version of the WPP Policy Book, Section 18 that are end-user-specific. Also included reference to the Kantar Privacy Policy and WPP Policy Book Section 24 on "Social Networking Sites and Blogging"	Ron Thompson	Matt Graham-Hyde (for the Oct. 6 release)	August 25, 2011
Revised "Security, Mobile and Portable" to mention the new Mobile Device Policy.	Ron Thompson	Matt Graham-Hyde	October 6, 2011
Annual review and approval by Kantar CFO	Ron Thompson	Robert Bowtell	July 12, 2012

Revisions	Editor	Approved By	Date
Annual review and approval by Kantar CIO	Ron Thompson	Matt Graham-Hyde	August 15, 2012
Modified to incorporate more appropriately the verbiage around Kantar vendors	Ron Thompson	Eric Drake	Feb. 25, 2015

Signature:
Eric R Drake (Feb 24, 2015)

Email: Eric.Drake@kantaritp.com



KANTAR

Information Systems Policy:
Acceptable Use of Information Technology
Current Release: February 25, 2015
Current Approval Date: February 25, 2015

Purpose: Define the acceptable and prohibited uses of information technology.

Scope: Applies to all Kantar operating companies, Kantar vendors who connect to Kantar networks or process, store, or transmit data for Kantar companies, and Kantar headquarters, regardless of legal entity status.

Editors: Kantar ITP Transformation Director and the Kantar CIO

Policy Owner(s): Kantar CIO and Kantar CFO

1. Policy:

As Kantar companies collect and process confidential client data, Kantar companies must conform to the Kantar Privacy Policy which can be found on https://insidekantar.com.

This Acceptable Use Policy reflects and upholds WPP policy regarding the use of information systems. All WPP policies can be found on http://inside.wpp.com.

EMAIL and MESSAGING

Access to the Internet and to digital messaging systems (e-mail, instant messaging, and other Company electronic messaging systems) will be made available to users at the discretion of the management of your Kantar Company. As with all Company information and communication facilities, Internet access and e-mail must be used responsibly. They are provided primarily for business purposes and not for personal use, although reasonable personal use will normally be granted at the discretion of your Kantar Company management.

Your Kantar Company and the Kantar ITP reserves the right to monitor and report on Internet, e-mail and instant messaging usage, including specific web sites accessed by individuals (where not prohibited by local laws).

Remember that digital messaging systems have the same legal standing as any other written communication and may be used as evidence in courts of law.

Business should not be conducted using personal e-mail accounts. Your Company must have access to all correspondence regarding its business, which may not be possible if personal e-mail accounts are used.

Email Forwarding: Automated processes to forward corporate emails to non-WPP email accounts or domains must not be used.

Kantar IT Policy - 1 of 7 - Confidential

The information contained herein is confidential and is the property of Kantar and must be held in strict confidence and properly safeguarded by the recipient at all times. Any authorized copy of this confidential information, in whole or in part, must include this legend.

Policy-Kantar-Acceptable-Use-3rdParty

EchoSign Document History February 24, 2015

Created:	February 23, 2015
By:	Ron Thompson (ron.thompson@kantaritp.com)
Status:	SIGNED
Transaction ID:	XKYDB6TQ2Z5TBXK

"Policy-Kantar-Acceptable-Use-3rdParty" History

Document created by Ron Thompson (ron.thompson@kantaritp.com)

February 23, 2015 - 3:31 PM MST - IP address: 198.178.234.30

Document emailed to Eric R Drake (Eric.Drake@kantaritp.com) for signature

February 23, 2015 - 3:31 PM MST

Document viewed by Eric R Drake (Eric.Drake@kantaritp.com)

February 24, 2015 - 7:30 AM MST - IP address: 198.178.234.30

Document e-signed by Eric R Drake (Eric.Drake@kantaritp.com)

Signature Date: February 24, 2015 - 7:31 AM MST - Time Source: server - IP address: 198.178.234.30

✓ Signed document emailed to Ron Thompson (ron.thompson@kantaritp.com) and Eric R Drake (Eric.Drake@kantaritp.com)

February 24, 2015 - 7:31 AM MST