Electronic Communications User - Guidance
Using your electronic equipment responsibly
Issued by Personnel & Development
June 2010

Introduction

We provide you with electronic equipment to help you do your job that includes PCs, laptops and other electronic devices, mobile phones and access to e-mail and the internet. We expect everyone using KCC equipment to use it responsibly and to take into account our policies and position as an employer at all times. This guidance is for anyone who uses KCC's electronic equipment and who has access to the KCC's network, including employees, agency staff or contractors. It will help you understand the standards expected of you as a user.

Risks to KCC

Whilst using e-mail and the Internet is often essential to do your job, it has the potential to expose KCC to risks of legal claims including:

- a defamation claim;
- a discrimination claim, whether on the grounds of gender, gender identity, race, disability, sexual orientation, religion or age;
- a breach of copyright claim;
- a breach of contract claim;
- a claim for breach of the duty of confidentiality;
- a criminal prosecution following the discovery of child pornography or unlicensed software (for example music files such as MP3s) on the network;
- a criminal prosecution or civil action following a breach of data protection legislation.

This is why we have developed clear rules for the use of our network and why we need to describe the consequences of misuse and the measures KCC takes to monitor compliance with the Electronic Communications User Policy, Information Security Policy, Virus Reporting Procedure, Social Media Guidelines and this guidance.

KCC Standards

If you are at all uncertain or unclear about any of the standards you should talk to your

Network Use

Don't:

- install or download software without consulting Information Services Group (ISG);
- download software or shareware from the Internet without consulting ISG;
- connect to KCC's network, a PC, laptop or Personal Digital Assistant (PDA) which is not KCC property;
- store personal client data on the system unless the storage is covered by KCC's data protection registration under the Data Protection Act 1998;
- fail to comply with the KCC's Information Security Policy and ICT Security Standard (for example, allowing another user access to your password or leaving a work station unlocked);
- allow KCC property, for example a laptop or PDA, to be stolen by not securing it when off KCC premises (e.g., by leaving it in a vehicle);
- engage in criminal activity such as denial of service attacks, fraud or spoofing;
- Store personal electronic documents on KCC equipment (e.g. photographs, video files/MP3, music files).

E-mail

Do:

- adopt a responsible approach to the content of e-mails, bearing in mind that e-mails often need to be as formal as any other form of written correspondence such as a letter;
- be aware that e-mails are disclosable in any legal action against KCC and e-mails which have been deleted by a user or from the network may be recovered;
- remember e-mail correspondence is not private as e-mails can be easily copied, forwarded or archived without the original sender's knowledge. When drafting any e-mail you need to bear in mind that it may be read by a person other than the person you send it to;
- keep hard copies of e-mails only where this is necessary for KCC records and manage electronic records properly;
- delete all personal e-mails and attachments when they have been read.

Don't:

- send e-mail messages that are abusive, malicious, discriminatory, defamatory about any person or organisation, or which contains illegal or offensive material or foul language;
- open attachments to e-mails from unknown sources;
- send or forward unsolicited bulk e-mail messages, chain mail or "spam";

- send e-mails with large attachments (1MB plus) to more than five users without consulting the ISG Service Desk;
- forward KCC messages to personal e-mail accounts (i.e. auto-forwarding) except with express permission.

Social Media Use (Facebook, Bebo, Twitter, Flickr, Blogging etc)

Do:

- use social media only during work hours if it is part of your job or work;
- ensure that you apply for a social media licence and authorisation (via your directorate communication lead) if using social media on behalf of KCC;
- know and follow the Kent Code, Electronic Communications User Policy and Social Media Use Guidelines;
- remember that all social media sites are in the public domain and you are accountable for any statements you make;
- be responsible and professional and consider how the information you are publishing could be perceived.

Don't:

- use your KCC e-mail account for non work related messages or updates from Facebook or other social networking sites.

Internet

Don't:

- visit, view or download any non job-related material from any Internet site containing illegal material (such as child pornography, obscene material or race hate) or other inappropriate material. Examples of inappropriate material include but are not limited to criminal skills, terrorism, cults, gambling, illegal drugs and pornography;
- copy or modify copyright protected material downloaded from the Internet without authorisation;
- subscribe to a non-job related bulletin board, newsgroup or any other similar Internet service without obtaining your manager's permission;
- enter into a contract via the Internet without following KCC's standard authorisation procedures. A contract entered into via the Internet is likely to be legally binding in the same way as any other contract;

- use the Internet for illegal or criminal activity, for example but not limited to software and music piracy, terrorism or the sale of illegal drugs;
- access instant messaging sites or information storage sites of any kind;
- conduct financial transactions, including online banking and auction sites (e.g. Ebay), without your line manager's knowledge/permission.

Do:

- limit your access to personal online email accounts such as 'Hotmail' to your workbreaks during the day;
- Make sure any personal use is limited and does not interfere with your ability to do your job.

A breach of the above standards is likely to be a disciplinary matter that could result in some form of disciplinary sanction including dismissal. KCC will also take legal action against anyone who is not a KCC user that breaches these standards.

Gross Misconduct

The following are examples of gross misconduct when using KCC electronic equipment, devices and facilities. You are likely to lose your job if you are found to be misusing our equipment in any of these ways:

- Sending abusive, rude, illegal, discriminatory or defamatory messages or material;
- Sending a bullying or harassing messages;
- Compiling or distributing chain letters either internally or externally;
- Sending confidential information without authorisation;
- Excessive personal use of e-mail or the Internet in work time;
- The introduction of a virus onto the KCC system resulting from negligent or malicious behaviour (e.g. onto KCC PC, laptop, email or downloading files from the internet);
- Misuse of e-mail, the Internet, Social Media or the system generally which results in a legal claim being made against KCC;
- Accessing illegal material or pornography on the Internet;
- Unauthorised copying or modifying of copyright material or material protected by any other intellectual property right;
- Unauthorised downloading of software or files;
- Use of the Internet for criminal activity;
- Hacking, or other breaches of the Computer Misuse Act 1990.

Personal Use

We permit limited personal use of equipment and the network provided:

- all e-mail messages are kept short;
- excessive time is not spent surfing the Internet for non work-related purposes or on KCC Noticeboards;
- personal use takes place during work breaks and there is no interference with your performance or with business use of the network;
- the use of radio, MP3, or iPod's is appropriate to the working environment and is with manager's agreement and does not cause interference to either the users or those around them.

We reserve the right to withdraw this facility if it is abused. You should not have an expectation of privacy when using KCC's network as all use is monitored in line with the law. If you want to ensure the privacy of any information you should use internal post and not email.

Working Away From Your Workbase (Remote Users)

You may sometimes need to use KCC equipment and access the KCC network when working remotely, whether from home, a non-KCC site or when travelling. The standards set out in this document apply wherever our equipment and resources are being used and the following additional standards also apply.

Do:

- be particularly careful to secure access to the network by using your password when working from home, in any non-KCC location or whilst travelling.

Don't:

- allow members of your family or anyone else to use the KCC network or KCC equipment.
- display confidential information on the screen of the device you are using at any time where it may be visible to others. (See Working at Home – Data Protection Guidance)

Monitoring

To minimise the risks to KCC described earlier and to maintain the effectiveness, integrity and security of the network, ISG monitors its use. Our intention is that any monitoring will be proportionate to the risks of harm to KCC and your privacy as a user will be respected as much as possible. Monitoring is carried out in the same way regardless of whether the user is office based or working remotely.

Any monitoring will be carried out subject to the requirements of legislation including the Data Protection Act 1998, the Human Rights Act 1998, the Regulation of Investigatory Powers Act 2000 and the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000.

Network traffic and the performance of the network is monitored. KCC uses a firewall, an anti-virus product, an intrusion detection system and other software to do so.

Specific monitoring and recording of information is undertaken as follows:

- anti-virus software monitors all communications but will only record and quarantine those which it identifies as containing a virus
- software monitors the content of e-mails
- software is used to monitor the content of e-mails or the content of Internet sites visited where KCC reasonably suspects, or has received a complaint, that a user is misusing the KCC's network and/or is not following the standards set out in this guidance
- software will prevent access to certain designated non work-related Internet sites, unless use has been agreed as part of your job, and a record will be maintained of sites visited.

Access to E-mails and Work Area

Your manager may where necessary, request to open and read your e-mails and documents in your work area if you are absent from work due to sickness, holiday or any other reason. If you plan to be away from work for any period of time you can make arrangements for access to your e-mails or other files in advance. Contact the ISG Service Desk for guidance.

General

You will be made aware of any changes to this guidance as they occur.

You should only access KCC's network if you have read and understood the standards expected of you.