

Acceptable Use Policy Governing the Use of Information and Communication Technologies (ICTs)



INTRODUCTION

This policy document explains Cordia (Services) LLP's policy and guidelines on the permitted use of ICT facilities and what action may be taken if this policy is breached.

This document replaces any previous policies relating to the use of ICTs.

This policy applies to you if you use any computers, phones, laptops or other computing devices for your work. The policy is explained in detail in the following pages. A summary is shown below.

The term ICTs is used throughout this policy and this is short for Information and Communication Technologies. ICTs include personal computers, laptops, mobile phones, BlackBerry smartphones and any other electronic devices provided to you for your work.

By using Cordia ICTs you are agreeing to the terms of this policy. When accessing local area network services the message box shown when you login also requires you to agree to the policy before using services.

Questions or issues relating to this policy or its implementation should be directed to:

Brendan Murphy
Head of ICT and Marketing
Cordia (Services) LLP
Blair Court
100 Borron Street
GLSGOW
G4 9XE
T: 0141 353 9020
E: brendan.murphy@cordia.co.uk

SUMMARY

The main aspects of this policy are:

- Depending on your job;
 - you may have access to the Internet and our email system, as well as external email;
 - you may have access to our telephone network;
 - you may have access to our local area network;
 - you may have access to mobile phones, BlackBerrys or other mobile devices.
- You will be able to access the Internet for personal use at no charge, but you will need to pay for private telephone calls if you make them;
- Apart from an emergency, personal use of the Internet and email facilities will be restricted to meal breaks and/or pre and post-

normal working day. You should be aware that these restrictions also apply to the use of personal mobile phones. The current acceptable use times are; Mon-Fri anytime before 930 am, 12noon-2pm, anytime after 4pm (3.55pm on a Friday). You must be in your own time when using the Internet or sending emails for your own purposes;

- Cordia's directorate and senior management team can choose to deny or withdraw Internet and/or email access at any time;
- Personal use is authorised at the discretion of management and must not interfere with the business of Cordia (Services) LLP.
- All Internet access will be automatically monitored with monthly usage reports issued to the Head of ICT and Marketing for review, and action by your line manager as appropriate;
- All email usage may be monitored with monthly usage reports issued to the Head of ICT and Marketing for review, and action by your line manager as appropriate.

POLICY ACCEPTANCE

If you currently use ICTs as part of your employment with Cordia, you are deemed to have accepted the contents of this policy document.

DOCUMENT CONTROL

DATE	CHANGE	REV	Author	Approver
Jan 2010	Draft policy	n/a	B Murphy	n/a
June 2010	Draft policy	1.0	B Murphy and ICT staff	L Norwood

1.0 INTRODUCTION

Overview

Cordia makes effective use of ICTs and these are critical to the success of our business. However, ICTs can expose us to a number of technical, commercial and legal risks.

This policy:

- Gives you guidance on the use of ICTs to ensure you minimise business risks;
- Explains what you can and cannot do;
- Provides you with information about the monitoring systems that we use;
- Explains what will happen if you fail to follow this policy; and
- Provides you with some guidance on how to help keep our systems safe and our networks working effectively.

The main aims of this policy are outlined in the next few paragraphs:

Productivity

You are allowed to make personal use of ICTs. However you must restrict this use to break times and times outwith your normal working day. It is important that you respect acceptable and reasonable use. Don't stream or download music or video files as these activities put an unacceptable strain on our network and could seriously disrupt our business. Do not use chatrooms or use any instant messenger services.

Reduce Legal Liability

This policy must be followed to protect Cordia and all users from legal liability relating to use of the Internet, email and telephone use.

Reputational Risk

Our reputation is vitally important to us as an organisation and is important to our clients and our suppliers. The reputation of Glasgow City Council, our main client, is also important in the eyes of the public.

This policy helps protect Cordia's reputation. Your use of our local area network, the Internet, email and telephone should not have a negative impact on Cordia in any way.

RESPONSIBILITIES

Managers and supervisors are required to:

- authorise use of ICT facilities
- ensure staff comply with this policy when using Cordia (Services) LLP ICT facilities
- monitor the use of ICT facilities
- assist in dealing with breaches in line with the guidance in this policy.

Users of Cordia (Services) LLP ICT facilities are required to familiarise themselves with this policy and to adhere to it at all times.

SCOPE

This policy applies to all Cordia (Services) LLP workers, including:

- Employees of the LLP
- Contractors
- Consultants
- Students
- Voluntary workers
- Modern Apprentices
- Skillseekers
- Any other person who has access to Cordia (Services) LLP ICT facilities other than those listed above.

This policy applies at all times, including

- Office working
- Tele-working
- Home-working
- Remote/mobile working.

2.0 GENERAL GUIDELINES

The reason you have access to ICTs at work is mainly to allow you to carry out your job and for Cordia to do business. However, we do recognise that work and home life are becoming increasingly inter-linked, especially when using ICTs. We have therefore tried to take this into account.

You must ensure that any personal ICT use follows the rules outlined below.

Inappropriate use includes:

- Sharing of Cordia's ICT resources (such as logon details, access to PCs, access to shared file areas etc);
- Unauthorised changing of someone else's password or access rights;
- Violations of or infringes on the rights of any other person, including the right to privacy;
- Creating or transmitting defamatory, false, inaccurate or otherwise biased material;
- Using Cordia's ICTs to actively engage in displaying, procuring or transmitting material that is in violation of sexual harassment policy or laws, hostile workplace laws or other legal policies;
- Transmitting of customer, partner or other business or confidential data;
- Distributing, disseminating or storing images, text or materials that might be considered indecent, pornographic, profane, threatening, racially offensive, abusive, obscene, terrorist or illegal;

- Undertaking deliberate activities that waste user effort or networked resources e.g. streaming video content; storing MP3 files on network drives; global email advertising the sale of personal items;
- Any activity that restricts or inhibits other users from using the system or the efficiency of computer systems;
- Any communication that encourages the use of controlled substances;
- Any communication relating to political parties;
- Any communication that uses the system for the purpose of criminal intent;
- The installation of applications without prior approval;
- The use of internet chat applications (e.g. MSN Messenger, GoogleTalk, Yahoo IM etc);
- Introducing any form of computer virus onto the network; and
- Illegally copying material protected under copyright law or making that material available to others for copying.

Internet Usage

By using the Internet, Cordia can connect to others, publicise ourselves and conduct business. You must ensure that you use the Internet in a safe and controlled manner. Inappropriate use of the Internet can create unnecessary risks to our business.

Inappropriate use includes:

- Accessing Internet sites that contain obscene, hateful or pornographic material;
- Using the Internet to perpetrate any form of fraud, software or music piracy;
- Using the internet to send offensive or harassing material to other users;
- Accessing or downloading copyrighted information in a way that violates copyright;
- Downloading commercial software or any copyrighted materials belonging to third parties, unless this download is covered or permitted under a commercial agreement or other such license and is approved in writing by the Head of ICT and Marketing;
- Hacking or attempting to hack into unauthorised areas;
- Undertaking deliberate activities that waste users' effort or networked resources; and
- Use of peer to peer file sharing applications, including applications to download and share music or videos over the Internet.

IMPORTANT

If you access inappropriate material by mistake, inform your line manager immediately and ask them to tell the Head of ICT and Marketing.

You must take care when conducting financial transactions or disclosing personal information when using web sites. It is your responsibility to protect your personal privacy and Cordia will not be held responsible for any financial, personal or emotional loss or distress caused.

The use of instant messenger applications is strictly forbidden.

Email

Email is extremely useful and important. Cordia sends over 114,000 email messages on a monthly basis and over 226,000 are received in a typical month.

Email sent from a Cordia address has a responsibility associated with it, as recipients will associate this email with the organisation as a whole. It is therefore extremely important that you use email professionally and with caution.

Inappropriate use includes:

- Use of email to conduct personal business;
- Use of email to send chain letters or joke or spoof emails;
- Forwarding of confidential work information to a personal email address (take authorised work home on encrypted USB drives);
- Transmitting copyrighted information in a way that violates that copyright;
- Accessing the mailbox of another user;
- Broadcasting unsolicited personal views on social, political, religious or other non-business related matters;
- Transmitting unsolicited commercial or advertising material; and
- Giving rise to an unauthorised contractual commitment on behalf of the organisation.

IMPORTANT

Please be aware of our reputation and the damage that can be caused to it through inappropriate email use. Please be careful when joining mailing lists or discussion groups using your Cordia email address and ensure that any organisations you are dealing with are reputable, established and have an operating history.

Telephone Usage

You may have access to both fixed line phones and mobile phones. Both types are included in this policy.

You are allowed to use telephones for appropriate business use. Cordia does recognise that, on occasion, you may need to use the phone for personal use. When doing this, you must ensure that you keep calls to an absolute minimum and, where appropriate, make these calls during your break times or before or after work. Calls made during the working day should be urgent ones only.

When making business calls, it is also important that these calls are kept as short a time as possible. Using the telephone to chat with your work colleagues is not allowed.

If you work in a client office on behalf of Cordia (eg a school or other office) you must get authorisation from the person in charge of that office if you want to use the phone. Do not use client telephones without authorisation and use them sparingly at all times.

IMPORTANT

Personal calls may be made in appropriate circumstances e.g. emergency weather situations; to check on a relative/dependant who is ill; to notify others of overtime arrangements; returning a call from relative/dependent etc. Wherever practicable, personal use should be within your own time, such as meal breaks and periods before or after the normal working day. Where this is not possible, calls should always be made in a way that causes minimum disruption to others. **No charge will be made for these calls.**

It is anticipated that from time to time you may make personal use of phones in other circumstances e.g. contacting your bank; arranging appointments etc. These calls **MUST** be made in your own time. Please use your own personal mobile phone if this is possible.

At no time should your friends or relatives phone you for a general chat. It is really important that you discourage this.

When using a Cordia issued mobile phone for chargeable calls you must dial your number and follow it with a *. On receipt of your telephone usage bill you will clearly see these calls and you can then arrange to pay for them.

General Local Area Network Use

All users are required to sign onto the Cordia network to access systems. You are required to change your password every 42 days. Passwords should be at least 8 characters long and contain three of the following: a number, a lowercase character, an uppercase character or an extended character.

Anti-virus software is installed on all machines however this does not mean that viruses cannot get through. You must be particularly careful when opening email attachments or when downloading files from the Internet. If you are unsure about opening any file you receive, contact the ICT Helpdesk immediately and they will help you (x29955).

If you receive an automatic message from your system telling you there is a virus issue, switch off your machine immediately and contact the ICT Helpdesk for further advice on what to do.

Intentionally introducing malicious programs onto the network will be considered a very serious offence and may be dealt with by disciplinary action.

IMPORTANT

You are responsible for ensuring that your ICTs remain secure. This equipment is expensive, complex and takes time to replace.

Where possible, ensure that your screen does not face a public view and that your PC account is locked when unattended. You are responsible for ensuring that your PC account is locked, even if you are only leaving your desk/workstation for a few moments. Pressing the **Windows Key + L** will lock your machine.

All portable equipment (e.g. USB flash drives, mobile phones, laptops, BlackBerries, iPhones) should not be left unattended in plain view whether in or outside the office.

Care must be taken in the security of equipment particularly hand held or mobile items. Avoid leaving computer equipment in your car. If your car is the most secure place to store equipment, for example when travelling with a laptop, then lock it in the boot out of sight.

All laptops must be encrypted (this will be done for you by ICT).

Cordia does not allow the use of personal USB pen drives within the organisation. Should you require to transfer data please ask ICT support staff for an encrypted USB pen drive.

Mobile workers

No ICTs should be left in the main cabin of a vehicle (personal or work) and should be securely stowed in the boot area of cars or vans.

Never leave ICTs unattended in public places or other offices.

ICTs should always be carried in the main cabin of aircrafts.

If you are a mobile worker, it is your responsibility to ensure you regularly log on to the Cordia local area network to check that your virus software is regularly updated. If you suspect that your virus software has not been updated for an extended period, contact the ICT Helpdesk (x29955) for more help and advice.

Other Security Issues

- Do not under any circumstances disclose any personal passwords to any other person.
- Do not impersonate another user when sending an email.
- Do not amend email messages received.
- If you identify a security problem, notify the Head of ICT and Marketing immediately.
- Take every reasonable precaution to protect Cordia's network from security issues such as computer viruses.
- Do not show or identify a security problem to others.
- Do not allow another person to use your network account.
- Under no circumstances should software be installed on ICT facilities except in accordance with any authorisation given by the Head of ICT and Marketing.

Appendix Two sets out important information security guidelines that should be applied at all times. Please familiarise yourself with the good practice outlined in this document.

3.0 PRIVACY AND USAGE MONITORING

General Guidelines

The ICTs discussed in this policy are important. Misuse of them can have a bad effect on Cordia.

You should have no expectation of privacy and therefore this must be kept in mind when using ICTs for personal use.

The Head of ICT and Marketing reserves the right to access, interrogate and monitor any service or data as he sees fit for the purposes of protecting Cordia or ensuring appropriate business use. This includes accessing an archive of all emails for each user.

We reserve the right to use appropriate electronic monitoring tools to monitor ICTs.

Internet Monitoring

On a monthly basis, the Head of ICT and Marketing receives an Internet usage report. This report lists the top web sites visited, blocked sites where users attempted to visit, sites visited within core hours and the time and duration of visits. This information is manually interrogated and any issues are raised with line managers for action through the normal Cordia disciplinary procedures.

The discovery of any unauthorised use may result in suspension of internet access and/or disciplinary action.

Email Monitoring

The Head of ICT and Marketing may monitor email usage by using recognised software to automatically scan all incoming, outgoing and internal email messages for viruses and for pre-defined content.

The discovery of any unauthorised use may result in suspension of email access and/or disciplinary action.

Telephone Monitoring

Within Cordia, telephone monitoring comes under the jurisdiction of the Head of People Development and does not form part of this policy.

Local Area Network Monitoring

On a monthly basis, the Head of ICT and Marketing will instigate a network search for image, movie and music files. These files will be deleted without contacting users.

The discovery of any unauthorised files may result in suspension of network access and/or disciplinary action.

4.0 POLICY BREACHES

If you fail to comply with or uphold this policy you may be subject to disciplinary action, as set out in Cordia's procedures manual.

Action may include:

- Loss of ICT privileges, including internet/network/email access;
- Disciplinary action up to and including dismissal; and
- Criminal prosecution, if appropriate.

This policy cannot anticipate every situation; therefore you are reminded to seek guidance from line managers (or the Head of ICT and Marketing) if there is something you do not understand or if you need more information.

If you suspect any breach of this policy by those around you, you must immediately report, in confidence, your concerns to your line manager or the Head of ICT and Marketing. Everyone has a duty to be vigilant to ensure that our organisation stays safe.

GUIDELINES ON THE USE OF ICT FACILITIES BY RECOGNISED TRADE UNION REPRESENTATIVES

ICT facilities may not be used for Trade Union Activities or in conflict with Cordia (Services) LLP's interests e.g. opposition to Board decisions, ballots for strike action, etc

OTHER RELEVANT POLICIES, REGULATIONS AND CODES

- Employee Code of Conduct
- Equality Policy
- Communication Policy
- Computer User Code of Conduct
- Harassment Policy
- Computer Misuse Act 1990
- Data Protection Act 1998
- Information Commissioner's Employment Practices Code and Supplementary Guidelines

5.0 EMAIL HOUSEKEEPING

Emails are automatically archived and are held for a period of ten years before deletion. Should you wish to retain messages, these should be saved in a suitably named folder in your **My Documents** folder. Please delete unwanted messages speedily.

There are currently three levels of mailbox capacity and these are; tier one – 50MB maximum; tier two – 100MB maximum; and tier three – exceptions greater than 100MB. If your mailbox exceeds the maximum size you will be unable to send emails though you may still receive them.

If you receive an email not meant for you, redirect it to the correct person. If the email message contains confidential information you must not disclose this. If the email contains inappropriate material inform your line manager or the Head of ICT and Marketing.

Do not open SPAM emails, simply delete these or move these to your junk folder if the facility to do this exists.

Do not send trivial email messages. These waste unnecessary time and resources.

Be polite when writing emails.

Use caution when revealing personal information such as your address or phone number (or those of others), either via email or on the internet.

Avoid sending excessively large email attachments (attachments over 2MB in size). These are typically photographs or movie files.

Do not use email to harass or threaten anyone in any manner, for example: the persistent sending of unwanted email may be viewed as harassment.

Use mailing lists in moderation: avoid sending messages to large mailing lists (such as whole departments or Cordia wide), unless the message merits such readership and has been approved by the Head of ICT and Marketing or another Cordia senior manager.

If you are going to be away from your office for a period of time, including holidays, **you must set** an “out-of-office” message, with an appropriate redirection rule. An example Out of Office message is included as APPENDIX ONE. It is important that your message tells the recipient who to contact during your absence from work. (These messages are often set up as you leave the office. Please be very careful of spelling and grammar mistakes as these give a bad impression of the organisation.)

All email messages must include an appropriate Freedom of Information footer. This is also shown in APPENDIX ONE.

DATA PROTECTION

Cordia holds and processes personal data and has responsibilities under the Data Protection Act 1998. We all have an obligation to help Cordia comply with our responsibilities under the act and you should exercise due care when holding, processing or disclosing any personal data.

The current data controller is Brendan Murphy, Head of ICT and Marketing.

APPENDIX ONE

Hi

I am out of the office and will be back in the office on Thursday 1 October 20XX. I will not read my emails during my absence.

If you require assistance please contact Jane Dow on 0141 353 XXXX or at jane.dow@cordia.co.uk.

Regards

Sally

If you have a freedom of information enquiry, please email it to foi@cordia.co.uk or phone 0845 270 1555. You can also use an online form at www.cordia.co.uk/foi