Rotherham Metropolitan Borough Council

Electronic Communications Policy

Human Resources April 2009

ROTHERHAM METROPOLITAN BOROUGH COUNCIL

ELECTRONIC COMMUNICATIONS POLICY

CONTENTS

1.0 Introduction

This policy addresses the use of electronic communications by employees and will apply to all employees and Elected Members of Rotherham Metropolitan Borough Council (RMBC), consultants, contractors and agents employed by RMBC and partner organisations provided with authorised access to the Council's equipment, systems or information.

It is every employee’s responsibility to:

- read and comply with the requirements of the policy and its appendices.
- report any breaches of this code e.g. misuse of e-mail, Internet, Intranet, telephones etc. either to their line manager or via the Council’s Confidential Reporting Code.

This policy can be made available in other languages and formats on request.

Every employee has a duty of care for equipment such as phones and computers that are provided for their use. It is expected that employees will take reasonable steps to maintain the security and safety of equipment. This includes not leaving equipment in view in unattended vehicles and storing it securely when not in use. Mobile phones must be secured by a PIN number to prevent unauthorised use if they are lost or stolen, the PIN number must not be written down or kept with the phone. The loss, damage or malfunctioning of any computer equipment or data storage device must be reported to the IT Service Desk.

Misuse or loss of communications equipment due to negligence will result in employees being requested to reimburse costs to the Council and may result in disciplinary action.

Whilst using the Council’s communications technology systems employees should also ensure they comply with the associated Council policies on Data Protection and Information Security.

Failure to follow this code may constitute a serious disciplinary offence, which could lead to dismissal. It could also lead to criminal or civil action if illegal material is involved or if legislation, such as the Data Protection and Computer Misuse Acts, is contravened.

1.1 Electronic Communications and the Law

The most relevant legislation regulating electronic communications are:

- The Data Protection Act 1998 (relating to the use of personal information)
- The Computer Misuse Act 1990 (relating to unauthorised access and creation or distribution of computer viruses)
- The Copyright Designs and Patents Act 1988 (which relates to unauthorised copying often referred to as software piracy)

Breach of any of the above can constitute a criminal offence. Where the Council believes a criminal offence has taken place, it has a duty to inform the Police. Using the Council’s facilities in any way to break the law will be considered as gross misconduct under the Council’s Disciplinary Procedure.

1.2 Content and Usage

Internet Access is restricted through the use of web filtering software which prohibits the majority of inappropriate or offensive material. The content of emails is also monitored for policy enforcement, messages containing either words or attachments which breach the policy are automatically blocked.

You should be confident that anything which you access or send meets the following criteria:

- There is a legitimate business need (other than mundane personal use described later in 2.1)
- That it is within the law and does not breach copyright
- That you have the authority to send the message (i.e. when committing the Department to a course of action)
- Communications must comply with the Council's Dignity at Work Policy.

General advice on e-mail etiquette can be found in Appendix 3. A template for 'Out of Office' messages is supplied in Appendix 5.

There have been a number of disciplinary cases relating to the sending and receiving of unsuitable messages. (See Appendix 1 for the type and content of material considered inappropriate). Be aware that the use of the Council's facilities for the sending or receiving of such messages is strictly prohibited, if you receive a message that breaches this policy please refer to paragraph 2.1.

1.3 Issue of Mobile Phones and other handheld technology

The criteria for the issue of mobile phones and other handheld technology will vary within each directorate, due to the nature of the service. Although the reasons for issuing mobile phones and other devices will depend on the requirements of the service, the principles of determining the need and benefits of issuing equipment should meet one or more of the following criteria:

- The issue of equipment will significantly reduce risk such that employees can be reached in the case of emergency.
- A measurable business benefit with regards to cost savings is gained through the issue of mobile phones and/or other devices.
- There is a clear business benefit resulting in enhanced customer service through better access.
- Sufficient legitimate out of hours contact is required to maintain cover and/or emergency contact for the service.

It is the responsibility of the appropriate manager to ensure that the criteria is met and that there is a clear business benefit and need for mobile phones or other handheld technology (e.g. BlackBerrys) to be issued within their budget.

Note: Should your role change and you no longer meet the above criteria your mobile phone and/or handheld technology (e.g. BlackBerry) will be withdrawn.

It is the responsibility of the senior managers of the Directorate to:

- Maintain an up to date record of the issue of mobile phones and other devices.

- Ensure that all employees issued with mobile phones and other hand held technology have received and signed acknowledgement of the Telecommunications Policy in relation to the use of mobile phones and other devices.

- Review the use of mobile phones and other devices to prevent excessive use via the monitoring officer in each Directorate.

- Review the issue of mobile phones or other handheld technology to ensure the issue criteria continues to be met.

- Ensure mobile phones and other equipment are returned when the user no longer meets the criteria, leaves the authority or is suspended on the grounds of misconduct.

- Ensure the appropriate risk assessment has been completed.

It is recommended that each Directorate identifies an officer as the point of contact for the administration of the above.

1.4 Procurement of Mobile Phones and Mobile Devices e.g. BlackBerrys

All mobile phones must be ordered through the Council's procurement process by the appropriate manager however Mobile Devices (e.g. BlackBerrys) must be ordered via the ICT Helpdesk. Handsets will be ordered from the contract network provider. Managers should note that the current minimum contract for handsets is two years. When ordering BlackBerrys, arrangements must be made with ICT for the set up of the handsets.

1.5 Home Working

The rules outlined in this Policy apply to any equipment and systems provided or accessible to you when working from home.

If you work from home on an occasional basis it is important that you are contactable to your internal and external customers. Arrangements should be made with your line manager and communicated with colleagues.

If you work from home on a permanent basis you should ensure that your alternative contact details are available to your customers and colleagues in line with the Home Working Policy. It is a requirement that employees whose role is home based and/or customer facing has either a dedicated Council telephone line or mobile phone.

COLLEAGUES MUST NOT REVEAL PERSONAL HOME/MOBILE TELEPHONE NUMBERS WITHOUT PRIOR PERMISSION FROM THE HOME WORKER.

Where access to voicemail is provided, you should check your messages regularly or you should contact your team on a regular basis to check for urgent messages.

1.6 Voicemail

Where you have access to voicemail, this allows callers to leave a message at the dialled extension if the call has not been answered within five rings (15 seconds). You should ensure that you record a personal message on your voicemail so that the caller knows they have reached the correct extension.

You will be notified via e-mail when you receive a voice mail.

You can dial into the system, both internally and externally, to listen to messages and administer your mailbox using a password. You should keep your password confidential and should not divulge it to anyone or keep it written in a readily accessible place. When you have listened to your messages, ensure that you clear your inbox.

When leaving the office, ensure that you divert your phone straight to voicemail. On your return you should deactivate the divert. Legitimate use of voicemail to take calls when trying to avoid disturbance, either in the office or at home, is permitted.

2.0 Personal Use

Occasional and reasonable use of the Council's Electronic Communications systems is permitted providing that:

- It is in your own time i.e. outside normal working hours.
- It does not interfere with work performance or divert you from your duties.
- It is not used for furthering outside business interests or for personal monetary gain.
- The use of the Internet conforms to all other requirements in this policy.
- Usage does not adversely affect the performance of the e-mail system or corporate network.

The only personal usage tolerated is in the following areas:

2.1 Email
2.2 Mobile Phones
2.3 Telephones/Faxes
2.4 Internet Access
2.5 Social Networking sites, Personal blogs
2.6 Unofficial Bulletin Board

2.1 Email

A minimal level of mundane personal use is tolerated. This use must be outside your working time. Be aware that emails are monitored and that personally sensitive information should not be sent. Messages should not contain anything that others may find offensive or distasteful. Examples of material that is not permitted are those with a sexual content, jokes or chain letters, a more comprehensive list is detailed in Appendix 1. Personal encryption of messages is prohibited.

If you receive messages which breach this policy then you should do the following:

- If you know the sender, reply advising them that Council Policy prohibits that type of message and ask them not to send any more similar messages.

- If the message is from another Council employee then contact your Line Manager or Human Resources Manager for further advice.

- If you are offended or upset by the message you should refer to the Dignity at Work Policy, discuss it with your Line Manager or contact your Human Resources Manager.

- If the message is from outside the Council and you do not know the sender then advise the Service Desk who can arrange to have messages from specified senders blocked.

Such material may for example not be identifiable until the e-mail is opened and in these cases, employees will not be held responsible provided that they report it immediately. These items should never be passed on to other Council or non-Council individuals.

2.2 Mobile Phones

If you are provided with a mobile phone you can use it to make personal calls subject to the following:

- Personal use should not be excessive and any private calls should be avoided in normal working hours unless deemed “essential”.

- When making a personal call place a * after the number to identify it even if it is a Vodaphone to Vodaphone call at zero charge. N.B. Although some calls show zero cost on the bill (i.e. Vodaphone to Vodaphone) they are subject to a ‘recharge’ sum and therefore should be reimbursed to the Council

- You must reimburse the Council the cost of all personal calls. If private calls are paid for via salary deduction and misuse is found to have occurred, adjustments will be made for excessive calls/phone bills and private calls not using * as above.

- Ensure that when using the text messaging facility you do not use inappropriate language or send offensive material.

- Irrespective of re-imbursement of calls employees should not use mobile phones or any other electronic communications equipment to further outside business interests.

- When employees receive their quarterly mobile phone bill, they will be responsible for identifying any personal calls and text messages. These calls and/or texts should be highlighted, costs calculated and the usage form completed with payment to Financial Services. The highlighted bill should be handed to your Line Manager. If no personal calls have been made, you should state no usage at the end of the bill and sign and date this and hand it to your Line Manager.

- Data relating to itemised calls will be forwarded to Internal Audit.

Private text messaging must be kept to a minimum and only used in emergencies. You will be expected to reimburse the Council for the costs of private text messages. The rules surrounding the use of electronic communications detailed in this policy also cover mobile phones and BlackBerrys including text and video messaging.

2.3 Telephones/Faxes

Personal use of landlines should not be excessive and any private calls should be avoided in normal working hours unless deemed “essential”. You will be expected to reimburse the Council for the cost of these calls in accordance with your section’s current administration arrangements. It is the manager’s responsibility to monitor private use of landlines and to ensure that arrangements are in place for the administration of repayment in line with current costs.

Excessive and/or abuse of personal use of Council telephones may lead to disciplinary action.

2.4 Internet Access

Limited personal use is tolerated outside of working time. Although every attempt is made to prevent access to unsuitable sites it is your responsibility not to access any sites containing unsuitable material (some examples are listed in Appendix 2). Be aware that all Internet access is routinely monitored and logged and sites containing unsuitable material are prohibited at all times. The downloading of information for personal use is not permitted at any time.

All Internet connections should be via the Corporate network. Under no circumstances should there be a dial-up connection through any other Internet service provider (ISP) such as Wanadoo, AOL etc.

2.5 Social Networking Websites, Personal Blogs etc

Social networking websites, blogs (personal diary accounts) and other such communication methods are useful tools for:

- promoting Council services e.g. libraries, museums via alerts e.g. “follow us on Twitter, Facebook” etc

- communicating with hard to reach groups e.g. young people, community groups etc.

- publicising events and news stories

- bringing people with special interests together e.g. theatre users who wish to discuss areas of common interest

Social networking sites are those which contain personal information about the respective individual and where social interaction between different parties takes place. These sites are becoming increasingly popular and whilst we cannot be prescriptive about what you do in your own time out of work, it is necessary for us to outline what we consider would be detrimental behaviour or written content on a site that could potentially lead to disciplinary action being taken against you.

This section of the Electronic Communications Policy applies to the content that you publish on the internet (e.g. your contributions to blogs, message boards and social networking or content sharing sites) even if created, updated, modified or contributed to outside of working hours or when using personal IT equipment.

2.5.1 Cautionary advice – Personal Use on Personal Equipment

The Internet and its social networking sites, blogs (personal diary accounts), message boards, forums and content sharing sites are open to all to view, therefore, for your own safety and protection, caution must be exercised when using such sites.

Anything that you publish, particularly personal information e.g. date of birth, address, photographs etc may be used by others either for illegal or nuisance purposes e.g. identity theft, spam e-mails.

Where you identify yourself as working in a public facing role that could be deemed contentious, such information could also give rise to unwanted attention from service users.

Any illegal activity which is posted on the Internet can also be viewed by the Police.

Employees of the Council are ambassadors for the service they provide and should be aware that any serious misconduct or criminal offences committed during or outside working hours which could bring the Council into disrepute may result in disciplinary action being considered.

Personal opinions should not be stated in blogs relating to official business. If a personal blog clearly identifies that you work for Rotherham Council, and you express any idea or opinion, then you should add a disclaimer such as ‘these are my own personal views and not those of Rotherham Council’. Please note that this does not preclude the Council from taking action in cases it considers misconduct.

2.5.2 Guidelines for use of social networking sites and blogs

The following applies to both employees who are provided with access to social networking sites, blogs or other such communications tools for work purposes and use of such tools in an employee’s personal time using personal equipment.

Employees must not:

- Reveal confidential information about Rotherham Council in online postings. This might include revealing information relating to the Council’s clients, business plans, policies, employees, Elected Members, contractors, financial information or internal discussions. This list is not exhaustive and you should think carefully before making any postings. Please consult your line manager if you are unclear about what might be deemed confidential.

- Criticise or embarrass Rotherham Council, its clients or employees in a public forum (including any website), whether in jest or otherwise. You should respect the reputation of the Council and the privacy and feelings of others at all times. If you have a genuine complaint to make about a colleague you should raise the matter via your line manager using the correct channels e.g. Dignity at Work Policy or Grievance Procedure. If you have a concern or criticism about the Council and its practices you should raise this via your line manager or the Confidential Reporting Code. If you have a complaint about a particular Council service that you receive, then the formal Council Complaints Procedure should be utilised.

- Post comments that may be derogatory or defamatory towards colleagues, Elected Members, clients or contractors or may be deemed to be intimidatory or constitute harassment, whether in jest or otherwise. This list is not exhaustive and you should think carefully before making any postings.

- Use bad language, innuendo, discriminatory statements etc. that could potentially bring the authority into disrepute.

- Publish film or photographs on the Internet of activity that may bring the Council in to disrepute e.g. undertaking an illegal activity whilst wearing an RMBC uniform.

- Publish photographs of children or vulnerable adults on the Internet (without prior consent) in breach of safeguarding legislation.

- "follow" members of the public using a RMBC account as this could be misconstrued. Rather it should be up to an individual whether they "follow" or "become a friend of" the organisation and its departments.

2.5.3 Request Process

To gain access to social networking sites please complete an ICT Change Request form detailing the business purpose for your request – click here

2.5.4 Conditions of access

In terms of a social networking site account e.g. FaceBook, Twitter, Bebo etc., the following conditions apply:

- The applicant(s) must already have a generic e-mail address e.g. Recruitment

- An account must be anonymous and not assigned to a specific person e.g. Marketing Dept

- Passwords must be shared for business continuity reasons

These conditions apply when using social networking sites for work purposes only.

2.6 Unofficial Bulletin Board

This is a non-work facility, provided for employees to post items of interest and personal items for sale on. This should only be used outside normal working hours and must not be used to operate or promote private commercial activities.

Care should be taken to ensure appropriate language is used when posting messages on the bulletin board as any messages could potentially reflect on the Council or its employees. You must not post messages which are obscene, or harass or intimidate another person. Words and pictures are capable of being defamatory, if they are untrue or ridicule a person, and can result in damage to that person or an organisation’s reputation.

Informality, especially on the “unofficial” bulletin board, may be felt appropriate but intent can easily be misconstrued.

3.0 Unacceptable Use

The accessing or distribution of offensive, illegal or unsuitable material is unacceptable and subject to disciplinary action and/or prosecution.

Offensive material is anything which is abusive, intimidating, malicious or insulting. The persistent abuse of power, or the belittling of someone, either in public or private, which makes them feel upset, threatened, humiliated, vulnerable or undermines their self-confidence, through the use of Information Technology is unacceptable and will be deemed to be bullying or harassment. The Council's Dignity at Work Policy gives a list of examples of what constitutes bullying and harassment. In the specific context of electronic communications please see Appendix 1 for examples.

Employees must not engage in:

- Posting information that may tend to disparage, threaten, or harass others on the basis of gender, race, age, disability, religion or belief, sexual orientation or national origin.

- Posting statements that are defamatory or information that is false or misleading concerning the Council or other organisations and their services/products.

- Distributing confidential or sensitive information about the Council or its service users that might compromise its confidentiality.

- Deliberately using email in such a way that it constitutes bullying or harassment.

- Originating or participating in email chain letters.

- Substantial personal use of email, including the transmission of large documents or programs which will add an unnecessary burden to the network.

- Sending jokes, games and other non-work related emails, in a "chatty" and informal style could lead to problems for both the Council and its employees – do not assume others share your sense of humour.

- Sending or receiving inappropriate material via e-mail (either within an e-mail or as an attachment) such as adult material (pornography), racism / hate, drugs, terrorist and violence, gambling, share dealing, paedophilia etc (unless specifically for work purposes).

- Receiving, archiving, storing, distributing, editing or recording sexually explicit material or materials of a disturbing nature using the Council's network or computing resources (Appendix 1 provides examples of what would be considered inappropriate materials)

- The use of Internet based email accounts i.e. Hotmail is prohibited unless a case for access has been approved.

The list above gives examples of the types of behaviour which constitute violation of the policy. This is not an exhaustive list and there may be other violations which are not listed here.

3.1 Misuse

Where misuse has been identified, employees need to be aware that disciplinary action will be taken. The following, although not an exhaustive listing, is an example of actions, which would warrant serious disciplinary action with possible suspension/dismissal and in certain cases potentially criminal prosecution:

- Employees accessing certain websites e.g. child pornography and terrorist sites for non-work purposes.

- Employees accessing and/or distributing materials of an unsuitable nature (please refer to Appendix 1 & 2) via e-mail or within an e-mail attachment.

- Defacement of the RMBC website and Intranet.

- Any involvement in ‘hacking’, virus propagation and spamming of the RMBC or any website or Contravention of the Computer Misuse Act.

4.0 Security arrangements and controls

Security incidents, including the following examples, must be reported to the Service Desk immediately:

- Where it is believed another person is using an employee’s ID/ password. Attempts to log on as another user will result in cancellation of e-mail and Internet access and may result in disciplinary proceedings. Internet passwords should not be disclosed to anyone else. Each Internet user is totally accountable and responsible for usage on his / her account: this is also applicable where users have one “log on” password that gives access to both Internet and e-mail.

- If an employee believes another user is accessing prohibited material.

- Construction of personal / business [non-RMBC] websites.

- The settings of the PC anti-virus software being amended or disabled.

- Employees engaging in ‘hacking’ activities into non-RMBC web-sites (serious disciplinary action may result).

- If an employee accidentally accesses a prohibited site – this should be reported to the Line Manager as soon as possible after the incident and details of the incident should be logged.
- Unauthorised devices e.g. i-pods, cameras, non-RMBC memory sticks, external hard drives should not be connected to RMBC computers as this poses a risk to the security of the Council’s network.

Any suspicious e-mails or attachments should not be opened or forwarded to others as they may contain a virus.

When using telephones, either landlines or mobile handsets, and whether for personal calls or in the course of your duties, you should take into consideration the location where you are making the call, whether or not it will distract colleagues and whether or not the nature of the telephone conversation is appropriate in front of colleagues and/or visitors to the Council. It is also important to be courteous and take into consideration that colleagues may not want to be interrupted by your telephone conversations.

Personal mobile phones should not be used during working hours unless necessary and should be kept on silent/vibrate when in the office.

5.0 Filtering and Monitoring

The Council has developed a range of measures for the use of this technology in order to protect the Council and its employees from potential litigation or complaint about inappropriate access and use of communications. Such measures already in place include:

- A filtering system which filters e-mails and images/attachments contained within e-mails of an unsuitable, offensive or illegal nature.
- A security system of filtering inappropriate Internet sites to prevent access and record attempts to access prohibited sites which are offensive and illegal.
- General monitoring of the extent of usage of all forms of communications, such as e-mail, Internet, telephone and fax usage which is reported to Line Managers on a regular basis.
- An e-mail disclaimer is automatically included in outgoing e-mails.

Monitoring is undertaken to:

- Provide evidence of business transactions
- Inform for training purposes and standards of service
- Access business communications e.g. to check e-mail etc when employees are on holiday or sick
- Prevent or detect unauthorised use of the Council's communications systems and/or criminal activities
- Maintain the effective operation of the Council's communication system including protection against viruses
- Ensure the Council's policies and procedures are followed.

Routine monitoring of the Council's communication can and does take place. Do not assume that there will be any degree of privacy for personal messages. Employees need to be aware that consent to such monitoring is a pre-requisite of using the Council's communications technology.

6.0 Leaving the authority

On leaving the authority you must return all equipment, including laptops, handsets (including SIM cards), chargers and hands free equipment (e.g. Bluetooth headsets). It is the Manager's responsibility to reallocate any equipment if required and contact Procurement to advise of the name of the employee who has taken over any mobile phone or BlackBerry or to arrange for return. Managers should note that return of mobile phone handsets may not be possible before the minimum contract period has expired.

Appendix 1

Offensive and Unsuitable Material

The following identifies the type of content considered inappropriate:

- Aggression including threats or violence, abuse or obscenities

- Material which promotes illegal acts

- Sexual advances, propositions, suggestive remarks

- Sexually explicit or pornographic material

- Discrimination of any kind including insults or “jokes” which are related to a person’s sex, sexuality, religion or belief

- Racist abuse including “jokes”, insults or taunts

- Offensive abuse, ridicule, “jokes” or name calling relating to a person’s disability

- Material which the person knows, or ought to have known, would offend a colleague with particular sensitivities, even if it is not explicitly offensive, e.g. religious views or beliefs, gender identity, sexual orientation etc

- Care needs to be exercised in the tone, language and content of any messages sent by or to other Council or external equipment i.e. text messaging

This is not an exhaustive list. There may be other material which is not listed here which is offensive or illegal.

In general terms messages should not be sent that are likely to cause offence to other employees or bring the reputation of the Council into disrepute.

Appendix 2

Unsuitable Web-Sites

Certain websites cannot be accessed as a filter controls the access to the majority of unsuitable sites; examples of such sites are detailed below along with other examples of unacceptable use:

- Accessing, displaying, downloading or disseminating threatening, obscene or pornographic material including sites that display full or partial nudity or depict/ graphically describe/display sexual acts, activity or content etc.
- Racism/Hate.
- Militancy & Extremist.
- Drugs - sites that promote or provide information about the use of prohibited drugs (unless for work related purposes).
- Terrorist/violence/weapons
- Gambling
- Internet auctions
- Games – downloadable entertainment or games, or playing games over the Internet
- Hacking - sites that provide information about or promote illegal or questionable access to or use of computer or communication equipment, software, or databases
- Share dealing
- Paedophilia
- Downloading files, software or videos from the Internet or e-mail system unless there is a business related use for the material i.e. software that may enable a Web page to be viewed correctly
- Downloading, using or distributing copyrighted material without proper authorisation
- Construction of personal / business [non-RMBC] websites
- Sending and requesting ‘junk mail’, fund raising requests or chain letters are banned.
- Saving data to Internet files [known as ‘X’ files] is not allowed.

Appendix 3

Policy on the Use of Electronic Communications: Checklist of Do's and Don'ts

Electronic communications have transformed the way we work. They improve efficiency, productivity, information sharing and customer service. But technology is moving at an increasingly fast pace and revised advice and guidance on the use of electronic communications is necessary.

A detailed document (Electronic Communications Policy) has been produced which brings together all the current advice and guidance under one policy. This is a checklist of what to do and not to do which should be read in conjunction with the full policy which is available on the intranet or from your Line Manager.

Usage of electronic communications is monitored and filtered to make sure that the facilities are not misused. Limited personal internet use is allowed outside normal working hours. All e-mail messages are recorded and management may, under certain circumstances, monitor specific usage and have access to mailboxes.

Access to web-site material containing adult material, racism/hate, drugs, gambling, terrorist activities, share dealing or paedophilia is banned at all times. Non-business sites such as entertainment, sport and travel should be limited to reasonable access during non-working hours i.e. lunch-time.

WHERE MISUSE IS IDENTIFIED, DISCIPLINARY ACTION WILL BE TAKEN UP TO AND INCLUDING DISMISSAL. MISUSE OF THE INTERNET, E-MAIL, TELECOMMUNICATION OR COMPUTER EQUIPMENT CAN CONSTITUTE A CRIMINAL OFFENCE. WHERE THE COUNCIL BELIEVES A CRIMINAL OFFENCE HAS TAKEN PLACE, IT HAS A DUTY TO INFORM THE POLICE.

Fax and Telephone (Landlines & Mobiles)

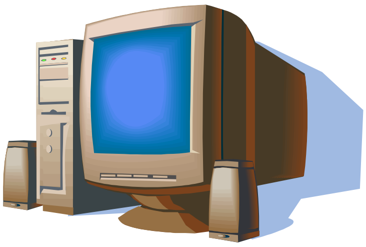
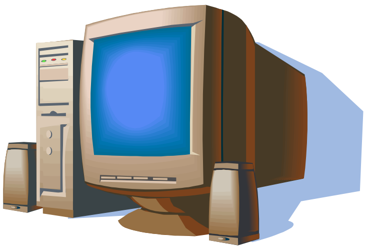
	DO • Answer telephones promptly and politely (internal & external) • Take messages accurately • Stagger lunch breaks and start or finish times to increase cover • Limit personal calls for emergencies only • Reimburse the Council for any personal calls made • Use landlines rather than mobiles if a cheaper alternative • Take care when disclosing sensitive or confidential information by telephone • Switch off mobile phones during meetings, presentations & when driving • Divert your mobile to the voicemail service when unavailable • Keep your mobile phone and SIM card safe at all times • Report your mobile phone/SIM card stolen or lost to your Line Manager • Restrict the faxing of lengthy documents wherever possible • Take care over the content, style and tone of faxes • Include a confidentiality statement on the cover sheet for confidential information to be sent
	DON'T • Make international and premium rate calls unless authorised • Make excessive private calls during work hours • Make or receive mobile telephone calls while driving on Council business without hands free kit • Use mobiles or BlackBerry devices during meetings as this can be a distraction to others • Send inappropriate or offensive messages using your mobile telephone e.g. text, video messages • Use private mobiles for Council business and claim reimbursement unless in an emergency situation • Send inappropriate text messages to another Council phone or external phone • Leave mobile phones unattended or in parked vehicles • Disclose sensitive, confidential information on a fax or over the telephone • Keep a personal identification number (PIN) in the same place as a SIM card • Use the voicemail system to 'screen' calls whilst in the office and available to take calls.

Electronic Mail (E-mail)

	DO • Keep messages short, clear and to the point • Ensure comments are accurate, justified and suitably worded • Use file compression software for large attachments – and ensure the recipient has the facility to open them • Check your mail box regularly and clear unwanted e-mails • Use folders to store items for efficient retrieval • Do not store messages unnecessarily either in Outlook folders or in personal folders – delete messages 'past their sell by date' regularly • Be aware that **all** emails can be monitored • Ensure the "out of office" facility is enabled for planned absence – click here for a template message • Use a Council recognised email signature format – employees and Councillors • Avoid taking paper copies of emails unless for correspondence files or meetings • Take care with language when posting messages on Unofficial Bulletin Board • Avoid "mail storms" – long discussions sent to a wide distributions list • Target your message - use distribution lists to send "all staff" emails rather than highlighting individual names • Beware of viruses • Remember emails have the same legal status as paper mail
	DON'T • Use all capitals or use gimmicks such as smiley faces or fancy fonts – this is very informal • Open any suspicious emails or attachments • Reveal your password to anyone else • Attempt to log on as another user • Read or send personal emails in normal working hours • Make excessive personal use of emails • Put your 'out of office' on whilst working at home • Read and post messages on the Unofficial Bulletin Board during working hours • Send sensitive or emotional messages • Send an email if it could embarrass the receiver or the Council • Send or request 'junk mail', fund raising requests or chain letters • Reply to SPAM (Slang term for unsolicited mail) • Send or import software programs by email or any other means unless there is a recognised business need • Use the urgent flag read receipt too often • Use the BCC and CC as a political tool when emailing colleagues • Import screensavers from outside the Council • Use inappropriate language or include abusive comments that can be interpreted as threatening harassing or insulting • Express personal views which may be misinterpreted as those of the Council • Distribute or store any material of a sexually explicit image or material of a disturbing nature via email or attached to an

	email

Internet and Intranet

	**DO** • Beware of viruses and follow security instruction and anti-virus procedures • Recognise **<u>all</u>** internet access can be monitored • Keep personal use to a reasonable level of access outside normal working hours, over lunch or after work • Use Council equipment for researching work projects and keeping up to date on developments • Talk to your line manager if you are unsure about any issues regarding access • Use the intranet to access Council policies and procedures
	**DON'T** • Access unauthorised web-sites / material • Use internet based email services e.g. 'Hotmail' • Download software onto your computer without authorisation • Disclose your password to anyone else • Disable or amend the settings of your anti-virus software • Attempt to 'hack' into any web-sites or computer systems • Construct non Council web-sites • Participate in non-professional chat services • Attempt to connect to the internet through any non-Council dial-up connection i.e. Wanadoo / AOL • Place documents on the intranet without prior authorisation • Illegally copy any computer software • Play games on the Internet • Introduce knowingly viruses to the Council's network • Induce or allow others to do any of these things

Appendix 4

Useful names and Contact Numbers

For IT Support - ICT Service Desk (33) 6300

For help on HR issues please contact the relevant HR Manager as detailed below.

2010 and Neighbourhoods and Adult Social Services	Odette Stringwell	(33) 4176
Children and Young People's Services	Paul Fitzpatrick	(82) 3786
Environment & Development Services	Julie Thackray	(82) 3726
Finance, Chief Executive's & RBT	John Vjestica	(82) 3707
HR Consultancy Team		(33) 4141

Appendix 5

E-mail Out of Office – Corporate Template

"I am currently unavailable until (date). If your enquiry is urgent, please contact (name & contact details)

When unavailable due to meetings:

"I am out of the office until (date/time as applicable). I will respond to your email when I return on (date/time as applicable). If your enquiry cannot wait, please contact (name and contact details)."