RTÉ

Technology Usage Policies

April 2011
Corporate Technology

Table of Contents

Introduction

Purpose

RTÉ’s information and technology investments must be protected from risks that jeopardize their availability, integrity and confidentiality. Therefore RTÉ has invested in information security technologies and put in place a set of Technology Usage Policies to ensure business continuity and minimise business damage by preventing and/or minimising the impact of security incidents in line with good practice as well as compliance with RTÉ’s legal obligations. This policy outlines the standards RTÉ requires users of its systems to observe, the circumstances in which it will monitor use of these systems and the action it can take in respect of breaches of these standards.

The Policy applies to all business processes used by RTÉ, wherever operated, and whether controlled by RTÉ or operated by a third party on our behalf.

The sections below deal mainly with the use (and misuse) of computer equipment, email, internet connection, telephones, Smartphones and voicemail but this policy applies equally to use of fax machines, copiers, scanners, CCTV and electronic key fobs and cards.

The Policy covers, among other things:

- material risks to IT;
- protection of information against unauthorised access;
- procedures to detect, recover from and guard against losses suffered, whether accidental or intentional, including error, fraud, malicious damage and disruption to, or loss of the IT infrastructure.

The purpose of this policy is to reduce RTÉ’s exposure to risks. It is incumbent on RTÉ personnel to be aware of their roles and responsibilities in using information and information technology resources and to ensure that all use is conducted in line with applicable laws, policies and standards.

Violations of any of these policies may lead to disciplinary action – up to and including dismissal in the case of employees and termination of contract and/or an action for damages or other legal proceedings in the case of non-employees. Any person who is aware of or observes a suspected violation of any of these policies is responsible for reporting the incident to his or her line manager.

This Technology Usage Policies document and associated documents are available on Marconi under the IT Helpdesk link on the right hand side of the front page.

Unless otherwise indicated, the term *information* should be construed broadly to mean both electronic and paper-based information that is used or created. It also refers to the information technology and systems used to create, process, transmit and store the information itself.

The term *personnel* refers to the managers and employees of RTÉ, as well as third parties acting at the direction of the organisation, (including contractors, consultants, agency staff and e-business partners) who have access to RTÉ's electronic communication systems.

Breach of these Policies and Guidelines

This policy is contractually binding and forms part of the terms and conditions of employment and/or engagement with RTÉ. All personnel using or accessing RTÉ technology resources are expected to observe the principles and spirit of these guidelines. Breach of these policies will be treated as a disciplinary matter for employees and subject to the normal courses of disciplinary action. Contractors may have their contracts terminated if found to have misused these policies.

Updating Procedure

This document is available on Marconi. The Marconi version will always be up to date and any changes to it will be highlighted by news items on Marconi or by Staff Information Bulletin.

Corporate Technology
April 2011

Use of Technology Facilities

General

Personnel are provided with Technology facilities, including access to the computer network, to assist them in the performance of their work. Data in RTÉ computer systems can be confidential or commercially sensitive. Personnel should be cognisant of their obligations in relation to the disclosure of information. This includes exercising due care in relation to the use of user codes / privileges and passwords, ensuring that screen displays are not open to view by others and that printouts are handled appropriately.

Computer accounts, passwords, and other types of authorisation are assigned to individual users and must not be shared with others. Users/Individuals are responsible for any use of their user account.

It is recognised that Technology facilities may occasionally be used for personal, non-RTÉ, purposes. Personal use is a privilege and not a right. Personal use should not be excessive, should not impinge on a person's work, and must not breach any of the policies and guidelines outlined in this document. This policy is dependant upon it not being abused or overused and RTÉ reserves the right to withdraw its permission or amend the scope of this policy at any time. In case of doubt, the line manager should be consulted. Please note that there should be no expectation as to personal privacy in relation to the use of the facilities.

RTÉ Technology facilities must not be used for personal commercial purposes or for storing, downloading or viewing indecent, obscene, pornographic (including child pornography) sexist, racist, hateful, defamatory or other objectionable, inappropriate or unlawful material.

It is important that those staff that have enhanced rights and privileged access to systems (e.g. Super users, Technology Staff, etc.) have further responsibilities to comply with these policies, particularly in the area of data protection (please see pages 19-20 below).

To facilitate good operational practices and also to ensure that RTÉ is compliant with its legal responsibilities, RTÉ business should only be conducted on RTÉ approved systems. To confirm whether a system is so approved please contact the IT Helpdesk on Marconi.

Under no circumstances should unapproved third party equipment or software be connected to, or installed on, RTÉ infrastructure or systems.

In the situation where there is a breach of these policies is believed to have occurred IT Helpdesk should be contacted in the first instance.

Acquiring New Technology

When new technology or applications are required for business purposes, Users are requested to contact the Technology Department within their respective IBD to ensure that the procurement and implementation processes encompass RTÉ's preferred technology platforms and security guidelines.

The IT Helpdesk

The IT helpdesk, accessible through Marconi, has been set up to assist users in resolving problems associated with approved technology.

Users should log all incidents related to technology problems with the IT Helpdesk.

The role of the helpdesk is to:

- Act as a single point for the logging of requests for assistance in the use of supported technologies and applications.

- Triage calls and resolve on the helpdesk where possible e.g. reset passwords for Peoplesoft.

- Refer calls to second line support for resolution and follow up on the resolution of issues.

If a user cannot access the Helpdesk, they should request a colleague to do so on their behalf.

Users can track the progress of their calls on the helpdesk. When a call is closed users will be notified via email. The facility to provide feedback is provided on call closure and all users are encouraged to do so.

Portable Computers

Laptops

The use of laptops in RTÉ generates extra security risks, particularly with regard to the loss of confidential information. The following guidelines should be observed where possible: –

- When travelling keep the computer with you at all times. This means declaring a laptop as hand luggage at airports.

- If left on the RTÉ campus, the computer should be powered off and stored in a secure cabinet or locked offices when not in use.

- Do not leave laptop computers unattended in relatively insecure locations, such as the back of a car.

- Do not display sensitive information in a public place where the screen could be viewed by others, such as on trains or in airports.

- Diskettes or other media holding sensitive information should not be held with the computer. Do not hold sensitive information on the hard disk unless it is encrypted to a standard agreed with the IT Helpdesk.

- Use a carrying case to reduce the risk of accidental damage.

- Observe any procedures outlined when you were provided with the computer – e.g. use of the power-on password.

- If the computer is used for remote access, do not use log-in scripts which contain passwords or other information of use to potential hackers. (For secure remote access facilities contact the IT Helpdesk).

- Ensure that backups are taken regularly.

- In the case of a computer which has been rented/hired or on loan to RTÉ ensure that all data is erased before it is returned to the supplier. This is a situation which mainly arises in the case of portable computers, but it is equally relevant in the case of desktop computers and servers.

- Theft of a laptop must be reported immediately to the IT Helpdesk by logging a ticket. If you are not in a position to log a ticket, please ring a colleague and ask them to do so on your behalf. This needs to be done as soon as possible in order to minimise security risks such as unauthorised remote access to the network.

- The majority of laptops in the organisation have been encrypted, however this should not diminish the importance of the policies/guidelines outlined above. Those in possession of non-encrypted laptops should take particular care with the nature of data stored on their devices so as not to present a risk.

- It is important that Laptop users periodically connect to the internet to ensure that they receive the latest AntiVirus updates.

Mobile Phones

Mobile phones are provided to staff to assist them in conducting their business duties for RTÉ. However in the course of this, from time to time, staff may use their RTÉ mobile phones for personal calls. When this occurs it is essential that such calls are reimbursed to RTÉ. Line managers who approve mobile phone bills for their staff are responsible for validating the cost of such personal usage. A Personal call reimbursement form is available for this purpose to recover the cost of any personal calls, SMS or data usage. Furthermore staff when travelling abroad for business purposes should ensure that, where possible, they use the local network which partners with our domestic mobile phone service providers. Telephone use is monitored through analysed billing. Any unwarranted or unreasonable use may be documented and may result in disciplinary action up to and including dismissal.

Smartphones*

The functionality of modern Smartphones makes their use more akin to personal computers rather than conventional mobile phones. As such, the same policies and guidelines apply to Smartphones as apply to Portable Computers. Additionally there are precautions required which are peculiar to Smartphones:

- If the Smartphone has password/PIN code functionality then it must be used;

- RTÉ SIM cards are not to be inserted into personal Smartphones;

- Line Managers in discussion with users should identify the appropriate data tariff required for the user;

- Smartphones are not to be used as Data Modems tethered to other portable devices e.g. Laptops. This is due to the data tariff on Smartphones not being suitable for heavy PC type usage. Such needs should be addressed using mobile data cards/modems.

A specific Smartphone request form is available on Marconi. There is also a link to this document in the appendices of this document.

Please see the detailed Smartphone Policy at the following location:

Smartphone Usage Policy

*(Apple iPhone, Android OS devices, Windows Mobile OS devices, etc.)

Software

Unauthorised Software and Copyrights

RTÉ is committed to the use of authorised software only within its computer systems. It is expressly forbidden for personnel to load or operate software obtained from the Internet, magazine gifts, or other sources unless their role specifically requires them to do this and with prior consultation with the Technology Department in the relevant IBD. The organisation is also committed to using software for which it has current licences and will not accept the use of more copies of a particular piece of software than it has licences or the connection of more than the licensed number of users to a multi user application.

It is forbidden for personnel to download unlicensed music, ebooks, videos or other media or to connect RTÉ computers to unauthorised peer to peer networks.

Software should only be installed or updated by authorised IT staff, following all licensing agreements and procedures.

The use of unlicensed software may expose RTÉ to civil and criminal liability to third parties. To ensure that computers remain compliant, the authorised IT staff and other staff authorised by RTÉ can inspect computers periodically to verify that only approved and licensed software has been installed. Any unsanctioned illegal or pirated software will be immediately deleted from the computer and the personnel responsible may be liable to disciplinary action up to and including dismissal.

Personnel are expected to comply with all relevant laws with regard to using information and network resources. Minimally, this includes honouring all applicable copyrights in both electronic and paper-based formats. Copyrights will apply even if there is no apparent copyright notice on the information.

If you have any queries in relation to this please contact the IT Helpdesk.

Software support.

RTÉ provides training and support in the use of supported packaged applications implemented to meet business requirements. The level of such support and the training approach are agreed as part of the original implementation project.

In addition, subject to agreement with IT, specific specialist software for limited use may be installed on the RTÉ network or accessed from within RTÉ. In such an event third party support arrangement must be agreed and may not be provided directly from IT.

It is the expectation that employees will have a general level of competency in the use of desktop operation systems and personal productivity software i.e. Windows and Microsoft office. Training in or support in the use of Windows or Office applications / macros, etc. is not provided.

Computer Viruses

It is the personal responsibility of all users to ensure that they do not introduce viruses into computer systems.

You should take care when receiving electronic information from an unknown source, including email attachments. (Word and Excel attachments could contain macro viruses).

In the interests of security, never launch or detach attachments that are not for business use. If you receive in particular, a file that 'looks suspicious', is from an unknown user, or contains macros or any file with a '.exe.' file extension, do NOT open the file. Contact the IT Helpdesk immediately to determine the best course of action.

All data imported on a computer (from sources such as CD, PDA, Memory Disc, floppy disk, USB Key, email or file transfer etc) should be scanned before use.

Users should not leave disks in their drives or boot (i.e. power on) with a disk since this increases the risk of infection by viruses.

Users should be aware that virus-scanning software is limited to the detection of viruses that have been previously identified. Users have a responsibility to verify that the virus scanning software they use is being updated on a regular basis (particularly for remote users) to maintain currency with the latest virus protection. To confirm that you have the latest virus software, please contact the IT Helpdesk

Always log off at the end of your working day or during prolonged periods away from your computer. If you do not log off, you may not be protected against new viruses.

If you have any doubts contact the IT Helpdesk immediately.

Policy and Guidelines for Internet Usage in RTÉ

RTÉ regards the Internet as a very valuable aid to the work of many people in the organisation. Appropriate security and usage policies and procedures must support this commitment to the Internet. It is in this context that this usage policy has been developed. It is designed to facilitate all Internet users within RTÉ to maximise the advantages of having access to the Internet while minimising the associated legal risks and practical hazards. Where appropriate, these policies also apply to the use of RTÉ's internal Intranet.

General Principles

Use of the Internet by personnel is permitted and encouraged where such use is suitable for business purposes and supports RTÉ's goals and objectives. Personnel are allowed to use RTÉ's internet facilities for limited personal use provided that such usage does not interfere with their work responsibilities and otherwise complies with these policies. The Internet should be used in a manner that is consistent with RTÉ's standards of business conduct and as part of the normal execution of an individual's job responsibilities.

Inappropriate usage could include visiting Internet sites that contain indecent, obscene, pornographic, sexist, racist, defamatory, hateful or other objectionable or unlawful material. The identification of inappropriate sites is further facilitated by an industry standard database of inappropriate websites, which is updated daily.

Monitoring

Overall access to the Internet is subject to monitoring and to this end RTÉ has implemented appropriate prevention software which will assist in ensuring that this policy is observed. Users are subject to limitations on the use of the Internet and RTÉ will attempt to block access to inappropriate websites. The fact that an internet site can be accessed despite the use of filtering software does not imply that personnel are permitted to visit that site.

For business reasons and in order to comply with its various legal obligations as an employer, internet use is monitored and RTÉ may collect and review internet account activity which will be reviewed by authorised staff for inappropriate and unauthorised use of RTÉ's internet facilities. RTÉ has also invested in software, which can help to identify and record instances of inappropriate images. Monitoring will only be carried out to the extent permitted or required by law and as necessary and justifiable for business purposes. This software will not be used to report on an individual unless approved by the relevant MD-IBD and RTÉ Group Secretary.

Exceptional usage

Exceptional Internet usage, for example where required for editorial research by programme makers or journalists, must be prior approved by the relevant MD-IBD or Executive Director. All requests for such access must be made to the Chief Security Officer and approved by the MD of the IBD concerned. The appropriate form for such access can be obtained from the Chief Security Officer

Internet users shall not:

- Leave their Internet access session open when it is unattended.
- Visit Internet sites that are inappropriate.
- Make or post indecent remarks, proposals, or materials on the Internet.
- Anyone receiving such material should advise their line manager immediately.
- Upload, download, or otherwise transmit software or any copyrighted materials belonging to parties outside of the organisation, or to RTÉ itself.
- Download any software for which RTÉ does not have a valid licence to use.
- Reveal or publicise confidential or proprietary information. This includes sending or posting RTÉ confidential files outside RTÉ or inside RTÉ to unauthorised personnel.
- Participate in any non-professional, or non RTÉ business related, chat services.
- Download any software or files without adhering to RTÉ's virus protection measures and procedures.
- Intentionally interfere with the normal operation of the network, including the propagation of computer viruses and sustained high volume network traffic that hinders others in their use of the network.
- Use the Internet for personal commercial purposes.
- Steal files or copy files without permission.
- Send or disseminate chain letters.

- Connect to websites providing pirated music, ebooks, videos or other media or use unauthorised peep to peer applications for downloading media.

Other Points to Note

Employees are required to report any suspicious activity.

Personnel must not circumvent the firewall by using modems or network tunnelling software to connect to the Internet. Personnel should not connect to the Internet via an Internet Service Provider (e.g. Eircom) without first disconnecting from the RTÉ network. (In the first instance, users must obtain approval from the IT Helpdesk for Internet access via an ISP). If you are concurrently logged on using a dial up account and using RTÉ's network, there is a risk that you may allow a third party to access RTÉ's network. This bypasses any firewall (security precautions) and would be considered a disciplinary offence.

Users should be conscious that some web sites employ techniques to track user preferences and track personal information using 'cookies' and other techniques. Some of these sites upload user information to the Internet without the user's knowledge. Please note that such tracking could be a source of embarrassment to RTÉ, especially if the material viewed is inappropriate or offensive.

Breach of this Policy

Personnel working at RTÉ terminals are expected to observe the principles and spirit of these guidelines. Breach of this policy, including accessing inappropriate sites as described above or the circulation of such materials, will be treated as a disciplinary matter and subject to the normal courses of disciplinary action – up to and including dismissal.

This policy will be strictly enforced as very serious potential criminal liabilities can arise.

Policy & Guidelines for Email and Social Media Usage in RTÉ

Communication by email is a publication, not a conversation. RTÉ must protect itself and its employees from legal liability and reputational damage arising from the misuse of email.

Acceptable use of RTÉ email

With the general upsurge in email usage, it is increasingly important that all RTÉ employees take steps to maximise the advantages which having access to email can bring, whilst minimising the associated legal risks and practical hazards.

There is a tendency for people to use email to communicate thoughts and ideas in an unguarded and informal manner that traditionally may not have been committed to writing. Within RTÉ, email has replaced much face-to-face and telephone communication but, contrary to popular belief, it is neither transient nor temporary.

The ease with which email can be copied, stored, and circulated makes it a permanent medium.

Emails are considered to be "records" under the terms of the Freedom of Information Act, which has applied to RTÉ since 1st May 2000. As such, RTÉ may be required to make them available to members of the public on request.

Far from being anonymous, email leaves an electronic trail from which it is very often possible to identify the source of a message. Additionally, users should be aware that the ‘delete’ key DOES NOT DESTROY THE MESSAGE sent. The delete key merely allows that physical area of the hard drive to be overwritten with subsequent messages, all of which can be ‘recovered’ by IT specialists if necessary.

Defamation and harassment actions, negligence cases, and claims in respect of the disclosure of trade secrets are just some of the legal actions that have recently been taken as a consequence of Internet and email activities in other organisations.

Defamation

In law, defamation comprises the publication of an untrue statement tending to lower the person involved in the estimation of right-thinking members of society generally or causing him or her to be shunned or avoided.

Liability for defamation applies to electronic communication just as it does to other forms of publishing. If an employee is the author of a defamatory message sent by email or of a comment published on social media, which is either unintentionally or inadvertently accessed by someone other than the intended recipient, he/she will be responsible for it and legally liable for any damage caused.

Sexual Harassment and Bullying

Just as it is unlawful for an employer or employee in the course of their employment to sexually harass or bully another employee, the sending of suggestive, sexually explicit or abusive emails or social media comments, can also constitute harassment. If such messages are received they should not be forwarded and should be reported to IT. If you are asked by the recipient of an email to stop sending personal messages then always stop.

It is worth remembering that, given the ability to forward messages, a single email may reach a much wider and more diverse audience than was intended when it was written. This serves to greatly increase the scope for causing offence. Likewise the publishing of such unacceptable content to social network sites is not acceptable.

RTÉ has a legal duty to protect its employees from harassment and must insist upon anti-harassment guidelines being observed in relation to email and social network usage and, furthermore, must insist upon the right to access all messages sent or received and also all content published to social media sites using RTÉ terminals.

Discovery & the Freedom of Information Act

Because email and social network sites represents a fertile source of potentially discoverable information in legal proceedings, it is important that everybody protects themselves by adhering to RTÉ's email and social networking policy with respect to message and published content.

The enactment of the 1997 Freedom of Information Act, which aims to ensure that the activities of public bodies are transparent by stipulating that their records are legally available to members of the public, makes this all the more pertinent.

Mass Messaging

Do not mass circulate messages unless you are absolutely satisfied that it is both:-

(a) necessary for RTÉ business purposes, and
(b) will not cause any disruption to the email system.

Mass messaging can cause serious disruption and expense to RTÉ.

Personal Use and Privacy

RTÉ allows employees limited use of its email facility for personal use, provided that such use does not interfere with their work responsibilities and complies with these guidelines. Employees making use of the RTÉ email facility are expected to exercise a degree of common sense and sound judgement in relation to what they write.

Monitoring

For business reasons and in order to perform various legal obligations in connection with its role as an employer, RTÉ may monitor email use and may to the extent permitted or required by law and as necessary and justifiable for business purposes renew, audit, intercept, access and disclose all messages created, received or sent over its email system.

Disclaimer

The following disclaimer will attach to all emails sent from RTÉ terminals to external addresses:-

"The information in this email is confidential and may be legally privileged. It is intended solely for the addressee. Access to this email by anyone else is unauthorised. If you are not the intended recipient, any disclosure, copying, distribution, or any action taken or omitted to be taken in reliance on it, is prohibited and may be unlawful."

While the disclaimer may offer some protection, this should not be considered in any way absolute. Observation of these guidelines, regardless of the disclaimer, is therefore, essential.

Worth remembering

- Consider your message a publication, rather than a conversation.
- Ensure that any information sent is true and accurate, or suitably qualified if you are not certain that what you are writing is free from error.
- Once content is published to Social Media tools, you have no control over who accesses such content, and how long the content will be retained
- Do not criticise colleagues or those for whom you have responsibility via email or social media tools.
- Avoid making personal remarks about others.
- Always remember that your email could become public knowledge through a subsequent court case or under a Freedom of Information Act request.
- Consider who your email must be sent to and avoid unnecessary copying. In particular, use "Reply to all" with great caution.
- Mark all commercially confidential emails as appropriate. Agree wording with Legal Affairs or a TV Lawyer as appropriate or consider an alternative way to disseminate the information.
- If you receive an email in error, return to the sender. If it contains confidential information do not copy, disclose or use that confidential information.

Good housekeeping

Passwords - Do not disclose to others.

Email window - Do not leave open on your PC when it is unattended.

Storage - Review your email regularly. Please delete any emails sent or received that no longer require attention and are not part of an ongoing project. This is in the interest of limiting the risk of inadvertent disclosure of sensitive data and of saving space on servers.

Inappropriate messaging – Do not use the email to send inappropriate messages or forward junk mail. These messages can cause annoyance and clog up the email system. The RTÉ Intranet system, Marconi, is a more suitable medium for disseminating information messages across RTÉ.

If you are on the receiving end of inappropriate messaging or social media content, please inform your line manager.

To minimise the risk of identity theft be mindful of the personal information published on Social Media tools.

Be aware of the threats of phishing and identity theft scams which attempt to extract personal details in relation to your personal online accounts (Banking, e-Government, etc).

Before sending

Check your mail for ill-considered remarks.

Before hitting your ‘send’ key, ask yourself if you would mind if someone other than the intended recipient read your message. If the answer is yes - DON’T SEND IT!

Webmail

The provision of external access to the RTÉ email system using Webmail presents special security risks. The following policies and procedures are designed to reduce the risks.

It is the responsibility of each person using external access email to comply with RTÉ’s policy on such access. You should adopt appropriate information security standards and guidelines to protect corporate information and corporate information systems against unauthorised access.

Protecting against unauthorised intrusion

Unauthorised access to your email could be achieved by someone getting access to your password. This could be through the use of insecure passwords or through social engineering – for example, being tricked into disclosing your password to someone.

Use of secure or strong passwords is essential.

When users enable their email account for external access the RTÉ password checking system checks that the password is of an appropriate strength. The criteria currently in use are that the password must be seven characters or more in length and a mixture of upper and lower case and numeric characters.

Suggested guidelines for a strong password usage:

- Don't use your login or user name in any form (as-is, reversed, capitalised, doubled, etc.)
- Don't use your first, middle, or last name in any form.
- Don't use your partner's, children's, friend's, or pet's name in any form.
- Don't use other information easily obtained about you, including your date of birth, car registration number, telephone number, personal public service number, make of your car, house address, etc.
- Don't use a word contained in dictionaries.

- Don't use a password containing fewer than eight characters.

- Don't give your password to another person for any reason – you are responsible for any use of your user account.

- Do use a password with at least eight mixed-case characters (upper/lower).

- Do use a password containing non-alphabetic characters (digits and/or punctuation)

- Do use a password that is easy to remember, so that you don't need to write it down.

- A useful tip in creating a strong password, is to think of a phrase and generate the password from the first letters of each word in the phrase. You can also substitute various special characters instead of letters e.g. ! for I, 0 for O, $ for S, € for E. (for C, @ for A, etc.

Change your password

You should change your password every 90 days.

When you change your password do not use a previously used one.

To assist in not having to remember multiple passwords, change all your passwords at the same time to your new password. For example, when you are prompted to change your login password, also change your Peoplesoft, Agresso, etc. passwords at the same time.

Attachments

When you open an attachment it is copied to a temporary directory on the PC you are using. Be aware of this, especially when accessing webmail on a non-RTÉ computer. You may want to clear the Browser's cache or temporary directory if you have viewed a document that you regard as confidential.

Log out when you have finished using your email account

The system will log you out of your account after ten minutes of inactivity but it is best to log out of the system by clicking the Logout button to the left of the screen. If you do not log out it may be possible for someone to read your mail and send emails on your behalf.

It's not enough just to use the back or forward buttons on the browser or to simply close the browser in order to log out since someone might still access your email. **Click the Logout button.**

Account lockout

If you enter the wrong password three times within 15 minutes the system disables your login for 15 minutes. You will see the following message on the login page.
"Your account has been disabled temporarily due to too many incorrect login attempts".

Note that this applies to both internal and external Webmail access.

The forwarding feature in Webmail

Since we can now access RTÉ email remotely there is no requirement to forward email outside RTÉ. Moreover, the storage of RTÉ email on the mail servers of other organisations runs counter to the security and operations policy of the Webmail external access system.

Acceptable use of Social Media

The last number of years has seen significant growth in the use of online social media tools such as; Twitter, Facebook, Bebo, LinkedIn, wikis, etc. These tools and websites now allow for easy self-publication and self-promotion and are designed to invite comment and reaction, much of which is publicly accessible.

RTÉ has no desire to censor the opinions of its staff. However, all individuals, whether staff, independent contractors or those who are associated with RTÉ should ensure that in using such tools that they do so in a manner that minimises risk to RTÉ and complies with RTÉ's policy on the Personal and Public Activities of Staff, which has been updated to reflect the proliferation of new social media tools.

This should be read in conjunction Chapter 7, Section 6 (4) of the RTÉ Staff Manual – RTÉ Staff and Politics, and Appendix 5 of the RTÉ Staff Manual - RTÉ Code of Business Conduct (Sections 7 & 12) and the relevant sections of RTÉ's Programme Standards and Guidelines.

Personnel must not post information on RTÉ business, comment on rumours or discuss confidential company information even if access to such information is limited to members of a private group.

Users must be mindful that information posted is not private and will often remain accessible for long periods of time.

At any time and without prior notice RTÉ may conduct automated searches of social networking websites for confidential corporate information or to monitor public discussion of the company.

Users who participate in online communication deemed not to be in the best interests of RTÉ will be subject to disciplinary action up to and including dismissal. Such communication can include but is not limited to sharing of confidential company information or posting inaccurate, distasteful or defamatory content about RTÉ or its employees in breach of RTÉ policies.

Users should report any negative or damaging comments about RTÉ to the Head of Corporate Communications.

Practices regarding the use of social media for the purposes of promoting RTÉ or RTÉ output may vary across the organisation. Staff and independent contractors are advised to consult with IBD guidelines and line managers as appropriate.

CCTV

A CCTV system monitors the premises 24 hours a day. This data is recorded and saved for 30 days save where an image identifies an issue and is retained specifically in the context of an investigation of that issue.

Data Protection

Introduction

The use by personnel and the monitoring by RTÉ of its electronic communications systems may involve the processing of personal data and is therefore regulated by the Data Protection Acts 1988 and 2003 as outlined below.

Data Protection is about your fundamental right to privacy and your right to access and correct data about yourself. The Data Protection legislation governs the collection, processing, retention, use and disclosure of information relating to individuals.

Data Protection Principles

RTÉ shall perform its responsibilities under the Data Protection Acts in accordance with eight Data Protection principles. They are:

- Obtain and process information fairly;
- Keep it only for specified, explicit and lawful purposes;
- Use and disclose data only in ways compatible with these purposes;
- Keep data safe and secure;
- Keep data accurate, complete and up-to-date;
- Ensure that data is adequate, relevant and not excessive;
- Retain data for no longer than necessary for the purpose(s) for which it is acquired.
- Give a copy of his/ her personal data to the relevant individual, on request

Responsibility

RTÉ requires all employees to comply with the Data Protection Policy. Failure to do so, e.g. unauthorised, inappropriate or excessive disclosure of or obtaining information about individuals, will be regarded as a breach of this policy and will be dealt with in accordance with RTÉ's Disciplinary Policy. If an employee is in a position to deal with personal information about other employees, he or she will be given separate guidance on his or her obligations, and must ask if he or she is unsure.

RTÉ collect and use information to provide the following services:

- A national television and sound broadcasting service which shall have the character of a public service, be a free-to-air service and be made available, in so far as it is reasonably practicable, to the whole community on the island of Ireland.

- Website and teletext services in connection with the services of RTÉ to enhance or improve your experience on our website.

- To provide online services. Each service has different information requirements. Therefore the information we need, and what it is needed for, can differ. For full details please refer to the terms and conditions for each service.

- To establish and maintain orchestras, choirs and other cultural performing groups in connection with the services of RTÉ.

- To establish and maintain archives and libraries containing materials relevant to the services of RTÉ.

- To assist and co-operate with the relevant public bodies in preparation for, and execution of, the dissemination of relevant information to the public in the event of a major emergency.

- Community, local, or regional broadcasting services, which have the character of a public service, and be available free-to-air (subject to the relevant consents etc).

- Non-broadcast non-linear audio-visual media services which shall have the character of a public broadcasting service (subject to the relevant consents, etc).

- Operation of one or more national multiplexes

- Exploitation of such commercial opportunities as may arise in pursuit of the services outlined above.

This policy was approved by the RTÉ Board, November 2009.

Inquiries about this Data Protection Policy should be made to Data Protection Officer, RTÉ, Donnybrook, Dublin 4.

Data Protection Guidelines

Data Owners (as defined below) are responsible for ensuring that Sensitive Personal or Commercial Data is processed in accordance with RTÉ's Data Protection Policy ("the Policy") and these Data Protection Guidelines ("Guidelines")

Data Owners are responsible for acquainting themselves with the Policy and Guidelines.

Data Owners are responsible for communicating and complying with the Policy and Guidelines in their own areas.

Where any aspect of the Policy or Guidelines is unclear or a situation arises that is not covered then clarification must be sought from the Data Protection Officer prior to processing the data.

Data Users (as defined below) should not process data in a way that is not sanctioned by the relevant Data Owners.

Central IT is responsible for approving the technologies and configurations that must be used in accordance with these Guidelines. Where specific technology guidelines are required they will be made available at: **Data Protection Documents.**

Prior to using any unapproved technology Data Users must first consult with Central IT.

Data Users of correctly configured and approved devices remain responsible for and must take reasonable steps to protect those devices whilst in their possession.

Data Owners / Users are accountable for behaving, in relation to the data under their control, in a manner that is consistent with the nature and quantity of that data.

Prior to processing any Sensitive Personal or Commercial Data the following questions should be asked and if the answer to any of them is "Yes" then consideration should be given to whether the processing is in accordance with the Policy and these Guidelines. If concerns arise then these should be addressed or escalated prior to proceeding.

- Is the data of a sensitive nature?
- Is there a large amount of data involved?
- Is the data being transferred/transmitted physically or electronically?
- Is the data being copied physically or electronically?
- Will the data processing be done in an un-encrypted form?

- Will any new copy or location of the data be subject to a lesser degree of security than the source copy or location?

- Will the data be processed by any new technology, system or process?

- Will any new copy or location of the data be outside of your control at any time?

- Will any new copies of the data remain after they have fulfilled the purpose for which they were created?

- Will persons not covered by these guidelines have access to the data as a result of your actions?

If you become aware of a data security breach, you must report it as soon as possible to the Data Protection Officer.

RTÉ requires all employees to comply with the Data Protection Policy and Guidelines. Failure to do so, e.g. unauthorised, inappropriate or excessive disclosure of or obtaining information about individuals, will be regarded as a breach of this policy and will be dealt with in accordance with RTÉ's Disciplinary Policy. If an employee is in a position to deal with personal information about other employees, he or she will be given separate guidance on his or her obligations, and must ask if he or she is unsure.

Definitions

"Data Owner"
Person(s) with responsibility for directing the data collection, processing and data storage activities of Data Users. (Note: a Data Owner may also be a Data User).

"Data Users"
Person(s), who directly or indirectly cause **Sensitive Personal or Commercial Data** to be accessed, copied, transmitted or transferred, physically or electronically.

"Sensitive Personal Data"

- Racial or ethnic origin, political opinions, religious or philosophical beliefs of an individual.

- Whether an individual is a member of a trade-union.

- The physical or mental health or condition or sexual life of an individual.

- The commission or alleged commission of any offence by an individual.

- The proceedings for an offence committed or alleged to have been committed by an individual or the outcome of those proceedings.

“Sensitive Commercial Data”

Privileged or proprietary information which, if compromised through alteration, corruption, loss, misuse, or unauthorised disclosure, could cause serious harm to the organisation owning it.

Practical Guidance Notes

Abide by the Data Protection Principles as regards obtaining and processing the data fairly and of keeping personal data only for the specified and lawful purpose.

In dealing with sensitive personal data you should evaluate the implications of storing it on a computer or word processor before doing so.

Do not disclose any personal data unless this disclosure is compatible with the purpose for which the data is kept. Note that disclosure can consist even of reading the contents of a computer screen to someone on the telephone.

Do not retain personal data on the computer or on removable media for longer than is necessary.

Always ensure that any personal data held is kept up-to-date.

Take appropriate security measures to protect the personal data. These include:

Storage Media including tapes, diskettes, CDs, DVDs, USB keys etc.

- Remove storage media from PCs etc. when not in use
- and lock them away.
- Reformat all storage media used to issue files of any sort to external
- companies or individuals, before copying the data.
- If storage media has been used for confidential data consult IT Helpdesk before passing them to someone else even though the files have been deleted.
- Always lock away archive and security copy storage media.
- Where storage media is given to another user, either within or outside RTÉ, you should keep a record of the transfer.

VDUs and PC Displays

- Log off and switch off during absences - coffee and lunch breaks and especially in the evening.

- Use physical locking devices where they are provided.

- Position VDUs to prevent the display being read by 'passers-by'.

Printers and Printouts

- Do not leave printouts lying around.

- Destroy all printouts which contain confidential or sensitive data – shred where possible.

- Remove printed listings and reports from printers immediately.

- Position printers to prevent reading by 'passers-by'.

Passwords

- Where password protection is provided use it in an effective manner.

- Change passwords and user codes frequently.

- Review user codes and access permissions regularly and change them when staff members leave or move to another department.

- Review activity logs and audit trails regularly.

Communication

- Ensure that procedures relating to the way in which access to systems is provided from outside RTÉ are observed.

- Do not leave modems connected to direct exchange lines or to PABX extensions unless it is essential to do so.

Commercially Sensitive Information

When dealing with commercially sensitive documents, the documents should be marked as such.

Emails can be marked “Confidential” through the Message Options – Sensitivity setting.
Other documents should include “Confidential” on each page of the document. This can be achieved through either a watermark or Header/Footer facility in word documents.

Journalistic Files

Section 21 of the Data Protection (Amendment) Act 2003 states that *Personal data that are processed only for journalistic, artistic or literary purposes shall be exempt* *from compliance* with Data Protection provided *the processing is undertaken solely with a view to publication of any journalistic, literary or artistic material.* What this means is that generally programme-makers' records of their research and production are not subject to Data Protection provisions. There is a public interest test which must be applied if a request is made for access to personal information held by programme-makers.

This exemption notwithstanding, it is important that journalists exercise all necessary caution in the storing of any personal information that may have gathered for programme-making purposes. This refers to in particular to the use to which that information is put, the accuracy of what is gathered and the actions taken to protect that information from being accessed by third parties.

Leaving RTÉ

Security of data

The following procedure should be followed when a person is leaving RTÉ to ensure that the email and other data in the person's allocated file space are handled appropriately.

The line manager must inform the IT Helpdesk two weeks before a member of staff leaves RTÉ. This will ensure that the security of IT systems and data can be maintained.

The person leaving should delete all unnecessary information from their file share (F: Drive) and their email before leaving. (The equivalent of tidying the filing cabinet).

When a person departs, their F: Drive and email and other system accounts will be disabled by IT. The user's data will then be deleted from the servers. Even in situations where a user returns on a later contract their previous data and rights will not be restored.

The line manager must apply in writing to the IT Helpdesk manager two weeks before the staff member leaves, to be given access to the person's F: Drive and email. The manager then has 30 days to review and file any necessary information to be kept. After 30 days all the user's data will be deleted.

Staff on planned leave of absence will have their accounts disabled immediately.

Staff on long term sick leave/maternity leave will have their accounts disabled after 3 months.

When a person leaves RTÉ their PC will be allocated to another person. Accordingly, it is important that the person leaving should delete any personal documents or files held on the computer.

Portable computers

Particular attention must be paid to data and software on notebook/laptop computers and PDAs when a person is leaving the organisation. It is the responsibility of the line manager to ensure that the ownership and confidentiality of RTÉ's data are preserved in these situations. There is an onus on all personnel leaving RTÉ to return all data, software etc which is the property of RTÉ.

Appendices

All the forms below can be found under the IT Helpdesk link on the right hand side of the Marconi home page. They are listed here below for your convenience

RTÉ Computer Access Form (to create a PC login and/or user email account)
Non-Personal Email request Form (to setup a programme/department email account)
Remote Access Request Form (to access RTÉ systems when you are off-site)
Wifi Application Form - Guest Account (for non-RTÉ employees/visitors to RTÉ)
Wifi Application Form - Employee Account (for RTÉ employees)
Laptop Request Form (to request authorisation to be allocated with an RTÉ laptop)
New Extension Form (to request a new phone number)

Monitoring Procedure

As outlined in the Technology Usage Policy users should have no expectation of privacy for the information they create, receive, store or transmit via RTÉ resources beyond applicable privacy and data protection rights. RTÉ reserves the right to monitor telephone, email, internet and other communication traffic. Monitoring will only be carried out to the extent permitted or required by law and as necessary and justifiable for its business purposes. The monitoring of individual user accounts requires authorisation by the relevant MD-IBD and RTÉ Group Secretary where there are reasonable grounds to suspect that there has been inappropriate use of the facilities provided. The Group Secretary will carry out a preliminary search and report back to the relevant MD-IBD. Where evidence of misuse is found, RTÉ may undertake a more detailed investigation in accordance with its disciplinary procedure, involving the examination and disclosure of monitoring records to those nominated to undertake the investigation and any witnesses or managers involved in the disciplinary procedure.