Email & Internet Usage

Reference: HR_POL_015
Version: 9.2
Owner: Carol McArthur
Author: Maggie West, 27 March 2019

Contents

1. Summary 3
2. Scope 3
3. References 3
4. Email & Internet Usage 3
5. Responsibilities 6
6. Records 7
7. Document history 7
Annexe 8

1. Summary

The HR Policy: Email & Internet Usage, details the way in which EDF Energy's email and internet systems can be used. The systems are provided for business use. At the Company and the manager's discretion staff may use the systems for personal use outside of working hours and in accordance with the HR Policy: Email & Internet Usage.

2. Scope

All permitted users of EDF Energy's information systems. Information systems include desk top computers, laptops and other mobile devices such as BlackBerrys and software authorised for use by EDF Energy.

3. References

Legislation, regulation and guidance from external organisations, including:

Computer Misuse Act
Copyright, Designs and Patents Act
Data Protection Act
ICO Data Protection Code of Practice
European Convention on Human Rights
Human Rights Act
Regulation of Investigatory Powers Act
Telecommunications (Lawful Business Practice, Interception of Communications) Regulations

4. Email & Internet Usage

4.1 Authorised use

EDF Energy technology systems, including access to email and the Internet, are provided and supported for business purposes. The company recognises that there are significant resources available on the Internet which can be used for work purposes and that it will be beneficial for some users to have wider access to these to support them in their roles. Wider access will be subject to business approval. All usage must be both reasonable and appropriate and in accordance with the Email & Internet Usage Rules in Section 4.3 and other company policies and procedures. Supplementary Guidelines for Trades Union Representatives on Internet and Email usage and the Sharing of Information is available on the Company Intranet.

Whilst EDF Energy accepts that it is not always practical to forbid all use of the system for non-business matters during the working day, this type of communication must be in accordance with any specific local guidelines and must be kept to a minimum.

Users may use the Internet and email systems for their personal use outside of their working hours, so long as this does not interfere in any way with their work or the Company's operational requirements. The use of these systems for both business and personal use is at the Company's and the manager's discretion and may be withdrawn at any time. EDF Energy reserves the right to block access to any internet site.

Any personal usage must not be detrimental to EDF Energy in any way and must not breach any term or condition of employment. All use must be in accordance with this HR Policy including the rules detailed below, the EDF Energy Code of Conduct and Bring Your Own Device (BYOD) Procedure and any other EDF Energy policies and procedures and must not place the user or EDF Energy in breach of statutory or other legal obligations. The Company assumes no liability for losses incurred whilst undertaking personal transactions on the Company's facilities.

The Company reserves the right to revise and update this HR Policy from time to time in order to reflect changes in the law, best practice, or the way in which EDF Energy conducts its business. The Company will consult with the recognised trade unions on any change to approach.

Additional supplementary information is provided by the Company in the Annexe to this document.

4.2 Monitoring, data protection and security

It is EDF Energy's policy to comply with all laws regulating computers and data protection. EDF Energy's Employee Privacy Notice and Third Party Privacy Notice set out how personal information is used and the obligations employees have to safeguard the personal data of others. Users must report any data security concerns or incidents immediately in accordance with the Incident Management Procedure set out in the Privacy Notice.

Users cannot expect privacy with regard to the email or computer systems usage. The Company may monitor, intercept and/or keep a record of any communication made on its systems (whether by email, Internet, telephone including Skype etc. instant messaging or otherwise) for a number of business reasons, including the following:

- For the purposes of establishing the existence of facts relevant to the business such as the details of particular transactions
- To carry out monitoring for the purposes of quality control or staff training
- To investigate or detect the unauthorised or inappropriate use of the Company's systems
- To support the management of company data (including employee, third party and customer personal data)
- To support compliance with relevant legislation and regulation To ensure the effective operation of the Company's systems
- In exceptional circumstances, checking users' email when they are away from the office to establish whether the mail is relevant to the business and to ensure that EDF Energy responds properly to its customers and other contacts.

Internet usage is traceable to the Company, the Company device and the user. The Company maintains logs of emails and other messages sent and received and websites visited by each individual.

EDF Energy operates software which aims to protect users and the Company's systems from access to potentially undesirable sites, files or software which pose an operating risk. If a user wishes to request that a site or file be made available for business purposes or a user becomes aware of an offensive or undesirable site that the security software is not prohibiting, they should contact the IT Service Desk. Users are also required to notify the IT Service Desk and their manager immediately if they receive inappropriate emails or if they mistakenly access a potentially offensive or undesirable site.

Users are responsible for taking reasonable steps to ensure that the security of the Company's assets and data are not compromised. Take particular care at non-EDF Energy locations such as vehicles, home, when travelling and in hotel rooms. Taking company equipment abroad may not be appropriate / allowed and could introduce additional risks. Advice can be provided by the Enterprise Information Security team and/or the Export Control team (EKI Export Controls) for those involved in controlled or regulated nuclear work. It is the User's responsibility to report to their manager and the IT Service Desk any damage, loss or theft of computing equipment provided to them. In the event that portable equipment, such as laptops, tablets and mobiles are known or thought to be stolen it must be reported to the police within 48 hours of discovery and a 'Crime Report Number' obtained.

Users must not attempt to damage the security of the systems, or infrastructure or equipment provided by the Company. Equipment should be made secure if unattended for any time. Passwords and other credentials must be kept secure and not shared. Appropriate measures must be taken to maintain the confidentiality of information that is transmitted via or contained in the Company's equipment, including the use of approved encrypted USB sticks. Care must be taken when using laptops in public places that no sensitive or confidential data can be seen by a third party.

4.3 Email & Internet Rules

The following rules are intended to protect both EDF Energy and the User. If a User is uncertain as to the application of any of these rules they should speak to their manager, the IT Service Desk or Employee Services.

1. The email and Internet systems must not be used in any way which may bring the Company into disrepute or damage the computing environment. All usage must comply with the Company's Code of Conduct and the policies and procedures on Equal Opportunities and Harassment & Bullying. Images, text or other material, which may be considered indecent, obscene or offensive, threatening, defamatory or generally inappropriate must not be downloaded, displayed, stored or communicated.

2. Company information must be managed in accordance with the EDF Energy Information Classification, Marking and Handling Code of Practice (and local interpretations where they exist). Information marked OFFICIAL SENSITIVE under the Government's Security Classifications must not be emailed outside of the accredited networks. Company information classified higher than OFFICIAL SENSITIVE must not be emailed at all. Additional guidance can be obtained from the appropriate Information Security Team.

3. Before any emails are forwarded outside of the company consideration must be given to whether this could give rise to any commercial or reputational risks or breaches of data protection. It will not be appropriate for users to forward information relating to the Company's business or other individuals to their personal email account unless it would be "NOT PROTECTIVELY MARKED" under the EDF Energy Information Classification Marking Handling Code of Practice. Business emails must not be automatically forwarded to external email accounts.

4. No illegal activity must be undertaken e.g. hacking or the sale of stolen or illegal goods.

5. Contracts or representations, on behalf of EDF Energy, must only be entered into by individuals authorised by the Company.

6. The following must not be downloaded or installed; unauthorised software, material that may damage the Company's IT environment or that of other organisations e.g. hacking tools or virus infected files; games, video, audio or music clips.

7. Licensing, copyright or other similar conditions must be complied with in respect of any materials downloaded or reproduced.

8. Users must not post on uncontrolled and open forums e.g. chat rooms, news groups.

9. External third party personal email service providers e.g. Gmail, Hotmail etc must not be accessed.

10. Company data including emails and attachments must not be stored by Users on the "cloud" or other external storage facilities such as Google drive, drop box or personal devices such as other computer or storage mediums unless on a system or application approved by IT such as BYOD.

11. Storage of pictures, video clips or audio clips are only permitted for business purposes.

12. The email and internet sites must not be used for gambling, sending chain letters or the operating of any employee's private business.

13. Unrestricted access to social networking sites such as Facebook, Twitter etc is limited to those with an approved business need.

14. EDF Energy email addresses and SMS numbers must not be used when accessing social networking sites for personal use. LinkedIn is considered a professional networking site rather than a social networking site.

15. Where Instant Messaging is approved for connection to services outside the EDF Energy IT systems, the personal use of the service for private discussions on public IM Services is prohibited.

4.4 Exceptions

In specific circumstances it may be necessary, for exceptions to this HR Policy to be made. For example, some Enterprise IT employees may be required to download software from the Internet as part of their job. The Industrial Relations & Reward Director, and/or the IT Operations & Programme Director (or their assigned delegates) as appropriate, must approve any exceptions.

4.5 Breaches

Non-compliance with this HR Policy will be taken seriously. Breaches made by employees will be dealt with in accordance with the appropriate disciplinary procedure. If the breach is serious it could result in the termination of employment. The Code of Conduct and Disciplinary Rules provide further information. In the cases of agency supplied workers or managed service workers, a breach may lead to the termination of their engagement with EDF Energy. EDF Energy may also report any security or criminal activity and may instigate civil proceedings.

5. Responsibilities

Role	Responsibility
Chief People Officer	Owns the HR Policy: Email & Internet Usage and is responsible for obtaining agreement to it from the Business Unit Human Resources Directors and those in equivalent roles in Corporate Functions and seeking approval from the Chief Executive.
Industrial Relations & Reward Director	Responsible for maintaining this HR Policy, ensuring that it is regularly reviewed and proposing any changes. Responsible for liaison with Enterprise IT regarding procedures to support this HR Policy.
IT Operations & Programme Director	Responsible for proposing any IT related changes to this HR Policy and identifying any internal or external changes, which may have an impact on the approach. Compliance will be monitored by the Company's IT software tools which will monitor Internet usage and email.
Business Unit Human Resources Directors and those in equivalent roles in Corporate Functions	Responsible for ensuring this HR Policy is implemented and communicated appropriately within their respective business areas. Make all users aware of the HR Policy: Email & Internet Usage.
Executive Members	Have been delegated authority to make decisions within their business areas in operating this HR Policy. Further delegation of authority within business areas will be captured in local governance documentation.
Enterprise IT	Utilising suitable monitoring software, maintaining logs and following up and reporting as appropriate.
Managers and Enterprise IT	Responsible for advising Human Resources of alleged breaches of this HR Policy.

Managers	Responsible for enforcing the HR Policy: Email & Internet Usage and where it is alleged that employees have breached it the appropriate disciplinary procedure will be instigated consistently.
Employees	Responsible for familiarising themselves with the HR Policy: Email & Internet Usage, adhering to it, raising any questions, requests or concerns they may have. Advising any contacts they may have, within or outside of EDF Energy, who have sent them any inappropriate material, of this Company policy approach.

6. Records

Appropriate records of email and Internet usage will be held by Enterprise IT.

Personal data will be retained in accordance with EDF Energy's privacy notices (www.edfenergy.com/yourprivacy).

7. Document history

Version	Date	Author	Comments
1.0	31/08/04	Maggie West	EDF Energy – Employment Policy Review
2.0	01/10/04	Maggie West	Updated: Executive Committee member responsibilities
3.0	01/12/05	Maggie West	Updated: Changes in IT organisation
4.0	01/07/06	Maggie West	Updated: Organisational changes
5.0	15/08/06	Maggie West	Updated: Equal Opportunities statement
6.0	14/02/07	Maggie West	Updated: Guidelines
7.0	14/07/07	Maggie West	Updated: Human Resources Director
8.0	05/04/11	Maggie West	EDF Energy – Employment Policy Review Replaces BE InfoComm IC/26/06 issued November 2006, BE ActionComm AC-1-2007 issued September 2007 and BE Information Management Security Guides - IM/L/SAS/SEC/005 and IM/L/SAS/SEC/007
8.1	06/07/12	Maggie West	Updated: Organisational Changes
8.2	09/10/12	Maggie West	Updated: Organisational changes & template
8.3	06/12/13	Maggie West	Updated: Annexe
9.0	04/10/16	Maggie West	Updated: Organisational changes and changes to Email & Internet usage rules and security
9.1	17/07/18	Maggie West	Updated: Organisational Changes and update to rules
9.2	27/03/19	Maggie West	Updated: Updates to orgz, records and review process

Annexe

Supplementary Information
Email & Internet Usage

The Email & Internet Usage Rules make it clear what is and isn't allowed when using the Company's email and Internet systems. The Company has monitoring arrangements in place to identify misuse. Incidents are investigated and, where appropriate, disciplinary action taken. If users are uncertain on any aspect of the Email & Internet Usage they should speak to their manager, the IT Services Desk or Employee Services.

It is important that Users understand the importance of information security when using the email and internet systems. EDF Energy's Code of Conduct states that employees must take appropriate steps to safeguard the security of company assets, systems and information. Laptops, mobile devices and company information should be made secure if unattended for any time. Company information is only to be stored on company approved devices and systems.

Taking company equipment abroad may not be appropriate / allowed and could introduce additional risks. Advice can be provided by the Enterprise Information Security team and/or the Export Control team (EKI Export Controls) for those involved in controlled or regulated nuclear work. Further information on the considerations for the country of travel can be found in the EDF Energy International Business Travel Security Procedure which provides information on Travelling with Information and Equipment.

EDF Energy's HR Policy: Social Media sets out the responsibilities that employees have in relation to their use of social media on Company systems, for work purposes and their personal use of social media.

Users should be aware that in accordance with the HR Policy: Email & Internet Usage there may be occasions when their usage, which may contain personal information, is legitimately accessed by the Company. The Company has processes in place to minimise this access. Logs are kept such that internet usage within EDF Energy is traceable to the Company device and the user. All emails sent and received within EDF Energy are archived in full. Whilst users are able to use the company's email and internet systems for personal use in their own time they should be aware that the support provided by the IT and Security teams are intended for business purposes. When the internet is used for personal use individuals must adhere (and where required agree) to the Website's terms and conditions of use in a personal capacity.

EDF Energy operates software which aims to protect users and the Company's systems from access to potentially undesirable sites, files or software which pose an operating risk. The software operated by the Company may be used as part of any investigation into potential breaches of the Email & Internet Usage and can identify the extent of any breach as well as the user responsible. Users should be mindful that increased use of the internet raises the risk of unintentionally exposing EDF Energy networks to malware and phishing attacks.

Users of mobile devices such as laptops and smart phones should be aware that there are potential risks of connecting to public Wi-Fi. Networks are not always legitimate and there is a higher risk of data being accessed. If you need to use a company laptop on public Wi-Fi then you will also need to connect to the Virtual Private Network (VPN) using your Global Protect/RSA Secure Token ID.

Further information on IT security can be found on Pulse – Facilities and Services - Security and Access.

The IT Service Point on Pulse provides useful information and is where requests for services and access to additional sites can be submitted.

Security concerns or incidents should be reported to the appropriate IT service desk on: 0333 009 7770 (Non-Accredited) 01452 653113 (Accredited); or to your local Information Security Team.

The following Best Practice Guidelines will assist all users to use EDF Energy's information technology systems effectively.

1. Always consider the most appropriate communication method and remember that the security and confidentiality of email is not guaranteed when transmitting data.

2. All emails should be concise and written in a professional way. All messages sent via email will be seen and legally viewed as originating on behalf of EDF Energy and should reflect our professional standards by using appropriate language. Remember that email is a formal method of communication and all emails, including those that have been deleted, can be recoverable and disclosable.

3. You should review the sender list and, if appropriate, check the recipient's details in the properties as it is remarkably easy for an email to be accidentally delivered to an unexpected recipient, particularly where there are users with the same name or when replying to a message

4. Do not send trivial messages or unnecessarily copy emails or "reply all" to recipients who do not need to see them. Emails should not be used as a substitute for face to face communication or communication by telephone, fax or regular mail, where these are more appropriate.

5. Very large attachments (10Mb and over) required for business purposes e.g. video clips, should not be forwarded via email. If there is a requirement to send large attachments, consider alternative mechanisms to do this such an approved encrypted USB stick. The IT Service Desk can provide advice and assistance.

6. Try to minimise the number of large attachments that are emailed to multiple email recipients as this will have an impact on storage. Consider other options such as using Sharepoint sites or converting PowerPoint documents to a PDF format.

7. Whilst we monitor all e-mails passing through our system for viruses you should exercise particular caution when opening unsolicited e-mails from unknown sources or an e-mail which appears suspicious (for example, if it contains a file whose name ends in .exe) and you should avoid clicking on links or attachments.

8. Do not send, forward or respond to chain emails, junk mails or jokes.

9. If delegated access permissions need to be assigned to an e-mail account ensure that they are set up correctly and that the permissions are reviewed on a regular basis to ensure they remain valid.

10. Good housekeeping procedures should be undertaken to ensure that stored data is not kept for longer than necessary. Some company files should contain a complete record of all relevant communications and so, where appropriate, copies of emails which need to be retained for record-keeping purposes should be transferred to the associated file from an individual's inbox.

11. Information obtained from the Internet can be unreliable – ensure the validity of the data when making decisions.

12. Close Internet browser pages when they are not being viewed. Their auto refresh updating facility places unnecessary usage demand on the IT systems.