An Roinn Dlí agus Cirt
agus Comhionannais
Department of Justice
and Equality

# Policy

# Acceptable Use of ICT Resources

## October 2018

## 1. Introduction

The Department's mission is to work for a safe and fair Ireland. We do this by striving to maintain community and national security, promote justice and equity and safeguard human rights and fundamental freedoms consistent with the common good.

Working with colleagues across the Civil Service, the Department of Justice and Equality (DJE) works to serve the State and the people of Ireland by offering objective and evidence-informed advice to Government, responding to developments and delivering Government objectives while striving to achieve optimal outcomes in the long-term national interest and serving citizens and stakeholders efficiently, equally and with respect, in a system that is open, transparent and accountable.

Information and Communications Technology (ICT) is a critical resource which supports the work carried out across the Department and its Agencies and refers to all the systems and services provided and supported by the ICT team. The ICT team is committed to providing a safe, secure and reliable ICT environment for all our users.

## 2. Purpose

DJE is committed to the correct and proper use of its ICT resources in support of its administrative and service functions. Inappropriate use of DJE's ICT resources could expose the organisation to risks ranging from virus attacks, theft and disclosure of information, disruption of network systems and services, damage to DJE's reputation, to litigation. The purpose of this policy is as follows:

1. To define the correct and acceptable use of ICT resources.
2. To state the standards of behaviour, interaction with and use of the ICT resources that is expected from users in order to protect the Confidentiality, Integrity and Availability of information and to protect the reputation of DJE and its staff.
3. To strike a balance between reasonable security controls and flexibility of operation.
4. To clearly communicate to users the purpose and circumstances under which their use of DJE ICT resources may be monitored, or their accounts and data accessed.

## 3. Scope

There is an obligation on all users of DJE's ICT resources to comply with this Policy.

This policy applies to:

- All ICT resources provided by DJE.
- All users of ICT including DJE staff, students, contractors, sub-contractors, associated agency staff, consultants and authorised third party commercial service providers.
- All personal and business related use of DJE's ICT resources.

## 4. Policy

While it is impossible for this policy to address all potential situations or events that may arise in our day to day work, good judgment should always be applied when using ICT resources. With this in mind, the following general guidelines should be observed:

- DJE ICT resources should not be used in a way that is likely to cause strategic, operational, reputational, or financial damage to DJE.

- ICT resources should only be used in a manner that is lawful and ethical.
- ICT usage should not interfere with the integrity or good reputation of DJE, or deliberately cause offence or harm to colleagues.
- Even though a particular action is not blocked or prevented by an ICT technical control, it may still be considered inappropriate and unacceptable by the Department and may therefore constitute a breach of this policy.

### 4.1. Acceptable Use of ICT resources

- Access to DJE's ICT resources is a business requirement and is not an automatic entitlement.
- All software licenses, copyrights and all other local and international laws governing intellectual property and online activities must be fully adhered to.
- DJE's ICT resources are to be used primarily for DJE business-related purposes. However, at the discretion of the line manager, occasional personal use may be permitted by a user provided it:
    - is not excessive and does not have a negative impact on DJE in any way;
    - does not involve commercial activities, such as running any sort of private business, advertising or performing work for personal gain or profit;
    - is lawful and complies with this policy and all other relevant DJE policies.
- The DJE has the final decision on what constitutes excessive personal use. DJE does not accept liability for any fraud or theft that results from a user's personal use of DJE's ICT resources.

### 4.2. Unacceptable Use of ICT resources

The following behaviours are unacceptable and prohibited when using DJE ICT resources:

- Using DJE's ICT resources for any unlawful purpose, to harass or defame, or to send, receive, download or view illegal, sexual, pornographic, racist, profane, abusive or other inappropriate material or messages.
- Using DJE's ICT resources for downloading, storing or distributing personal files (other than for incidental use as described above). DJE does not accept responsibility for any personal files or other content stored on its ICT resources.
- Unless instructed or authorised by ICT Division, the following actions are prohibited:
    - Attempting to download or install any software on any DJE desktop, laptop, server or network device.
    - Altering the hardware or software configuration of any DJE ICT resource
    - Connecting any computing devices, storage devices, printing or copying devices, cameras, mobile devices, modems or network equipment to any DJE ICT resource,
- Using any DJE ICT resource with the intention of bypassing monitoring or control systems, to gain unauthorised privileges, or to exploit any security weakness.
- Making unauthorised copies of licensed software or other copyright protected media.
- Third party or web-based personal email accounts (e.g. Gmail or Hotmail) are blocked and must not be accessed from the DJE network.

### 4.3. Confidentiality and Privacy

In order to fulfil the Minister's responsibilities, DJE necessarily processes personal data of customers, staff and third parties. The principles of Data Protection are particularly relevant to the use of ICT resources and users are referred to DJE's Personal Data Processing Policy in this regard.

- Personal data stored on DJE systems must be accessed by staff only in accordance with defined business need.
- Confidential, sensitive or personal information must not be transferred to non-DJE computers or storage without the appropriate authorisation at a minimum level of AP.

- Any files, digital communications or other records may need to be disclosed on foot of legal discovery requests, Freedom of Information requests, or Data Subject Access Requests (under data protection legislation).
- DJE is required to ensure the security, and prevent the abuse of, its ICT resources. Consequently DJE reserves the right to routinely monitor, log and record any and all use of its ICT resources for the purposes of:

    - protecting and maintaining network system security
    - helping to trace and resolve technical faults,
    - maintaining system performance and availability,
    - investigating actual and suspected security incidents,
    - preventing, detecting and minimising inappropriate use,
    - protecting the rights and property of DJE, its staff and other stakeholders,
    - ensuring compliance with DJE policies, current legislation and applicable regulations.

- This monitoring will alert the ICT Division to any unusual usage, which may be notified to the line manager and escalated to ICT Management for further and specific investigation. In the event that an individual's ICT usage or activity is subject to investigation they will be advised by HR Division.
- DJE also reserves the right, in exceptional circumstances, to take whatever actions it deems necessary and proportionate to protect the ICT resources under its control, and the users of those resources. Subject to ICT Management approval, this may include accessing user accounts, workstations or files, disabling user accounts or restricting user access, in particular where ICT operations, or other functions of the Department are likely to be seriously obstructed or damaged or where there could be security, safety or financial implications.
- The Department retains ownership of all computer files, documents and digital communications created, transmitted or downloaded by users in the course of using DJE's ICT resources. Therefore, there can be no expectation of an absolute right to privacy arising from your use of DJE's ICT resources.

### 4.4. User Accounts & Passwords

In order to prevent unauthorised or malicious access to information, DJE implements strong user account and password procedures to ensure that the information held is protected by the use of unique user accounts and passwords. All users must understand that they are responsible for all activities performed on any of DJE's ICT resources where your user account(s) and password(s) are being used.

- Only use the individual accounts that have been assigned to you; you must not attempt to access the ICT resources of another user.
- Do not write down your password(s).
- Do not re-use old passwords and do not use the same password across multiple accounts. You should have a unique password for each account.
- Immediately change any password given to you by ICT Division to a password of your choosing.
- Where possible, ensure to choose a username and password that is easy for you to remember, but difficult for others to guess. DJE systems will implement minimum password criteria.
- Ensure that all passwords created by or assigned to you are kept confidential at all times and are not shared with others including your colleagues or third parties, or stored on-line.
- Log off or lock your account/ ICT device when you have to leave it unattended and power it down at the end of the working day.

### 4.5. Mobile or Portable Devices

Subject to business need and approved at a minimum of AP level, staff may be issued with mobile devices such as smartphones, laptops, tablets, or portable storage devices. Because of their mobility, these devices pose particular security risks, most obviously the possibility of data loss or theft. Any loss or theft of data or portable electronic device must be reported to ICT Division helpdesk@justice.ie within 24 hours using the appropriate form.

Any staff who are issued with mobile devices will be bound by the latest version of DJE's Mobile Device Policy and the Remote Access Policy. It is your responsibility to acquaint yourself with any updates or amendments to these policies.

### 4.6. Email Usage

Email is one of the main forms of Digital Communications used across the department by staff to conduct their day to day business and DJE provides each member of staff with an email account to assist them in this. Email is also one of the main mechanisms used for the distribution of malicious software and continues to be a constant ICT security threat that requires robust control and filtering mechanisms, as well as user awareness, to protect the integrity of DJE's ICT resources. All emails (inbound and outbound) are monitored, emails are automatically backed up and can be restored, even if they have been deleted from your individual account.

- Emails that are considered to be records for the purposes of both the National Archives Act and the Freedom of Information Acts (those of "enduring organisational interest") must be filed in the appropriate document library and/or in hard copy file and not in your email account.
- You must be aware of the particular requirements about the transmission of personal data in line with the Personal Data Processing Policy.
- Your Department email address must not be used for subscription to social media platforms, on-line forums, discount or mass marketing sites.
- As you must not share your password, the "delegate" function must be used if others require access to your email or calendar.
- All users are required to use Department email systems for official business. The Department provides a secure remote access service to staff who require access to Department systems including email outside of work hours.
- DJE mail must not be automatically forwarded to personal email accounts.
- Access to web-based emails is restricted by the Department's security infrastructure.
- Where a non-official email system is required to be used in exceptional circumstances, staff and other service users should take particular care not to communicate confidential or sensitive information including personal data. The user must ensure a copy of any record is made available to the Department by copying the message to a valid Department account when sending the email.

### 4.7. Internet Access

The Internet is a valuable business tool to facilitate communication, education and learning, information sharing and authorised research. However, internet websites and the public networks over which internet communications travel cannot be considered secure. In order to minimise risk and to ensure best practice when using the Internet, DJE have set the following safeguards and procedures in place.

- Access to the Internet from DJE's network passes through web filtering systems and firewalls; you must not attempt to bypass these network security controls.
- ICT Division blocks access to sites/material that it considers may compromise the security of the DJE's network or is deemed to be inappropriate content on the network. Any attempts to

access websites in these categories will result in you being presented with an information screen informing you that access has been denied.

- In circumstances where you have a legitimate work-related reason to access filtered internet content, you may, with the approval of your line manager request access to such content for a specified period of time. Access requests must be submitted, supported by a business case in writing, through your line manager to ICT Division helpdesk@justice.ie.
- The technical security controls applied to different ICT resources, particularly mobile devices, may vary. However even if access to a website is not blocked from a particular device, it may still be in breach of what the Department considers acceptable use and may therefore be considered a breach of this policy.

Your usage of the Internet, including sites you visit or attempt to visit, and the frequency and duration of such visits is automatically logged by DJE's web filtering system. These logs are retained for a period of time after which they are deleted.

It is the general policy of DJE that you should not access the Internet (including the World Wide Web) for non-business purposes. However, some personal use will be tolerated provided that it is confined to break times and that it is not used to access, view or distribute (internally or externally) material which could in any way be considered offensive or inappropriate.

### 4.8. Social Media

The inappropriate use of social media has the potential to damage DJE's reputation as well as those of other individuals or groups. The negative impacts of that damage can be destructive and hurtful for individuals and the communities we serve. Consequently, DJE must adopt procedures that minimise the risks and follow best practice in the way individual staff members use Social Media.

Social media has significantly broadened the visibility of staff in the DJE. It is important to bear this in mind when using social media and to consider the content of your posts in the context of your position within the Department. It is particularly important to note that this is not limited to the use of social media during working hours, but also applies outside of working time. Conduct on social media should mirror conduct in the workplace, i.e., behaving in a respectful and responsible manner at all times.

You will not be provided with access to Social Media from the DJE network during core working hours unless there is a legitimate business need.

When engaging with social media in the course of business or in a personal capacity as a serving civil servant the following are strictly prohibited:

- Making distasteful statements or comments, or using language which can be deemed discriminatory on any grounds e.g. race, religious belief, sexual orientation, gender or disability
- Criticising DJE or its employees
- Making remarks about stakeholders
- Sharing sensitive and confidential information
- Encouraging or condoning violence
- Public debate on matters of local or national political interest
- Posting content from a DJE email address to any newsgroups or social media sites, unless posting is in the course of business duties.
- Any Social Media accounts or groups that are managed by staff on behalf of DJE remain the property of DJE. Control of any such accounts, groups etc. must be relinquished to DJE on request.

It is important to remember that once content is published online, it is very difficult to remove it. Further, although privacy settings may be activated, nothing on the internet is ever truly private. With this in mind, you are advised to think hard before posting anything online. If you are in any doubt as to the appropriateness or accuracy of any content you wish to post, it may be safer and more responsible to refrain from doing so.

DJE may from time to time make other communications or messaging systems available to users. These could include collaboration tools, instant messaging, social business tools, etc. Appropriate use of all of the above outlined systems must be appropriate and in line with this policy.

### 4.9 Information Backup

ICT Division only backup network drives on DJE's servers. Your local storage drive (typically the "C drive") will not be backed up therefore you must not store 'business critical' information there. Cloud-based services such as iCloud, Dropbox or Google Drive must not be used for the storage and backup of DJE's data.

Portable storage devices, such as USB drives etc. are also not backed up and must not be considered appropriate for the long-term storage of DJE data that is not otherwise stored and backed-up.

## 5. Roles & Responsibilities.

### 5.1. Responsibilities of Human Resources (HR) Division:

- To retain overall ownership, publication and dissemination of this policy.
- To provide support to users and line managers in the enforcement of the policy.
- To carry out investigation of suspected breaches of the policy and apply any disciplinary actions, if appropriate.

### 5.2. Responsibilities of ICT Division:

- To provide, deploy and manage ICT resources for DJE and all related training, advice and guidance to users.
- To put appropriate technical and other safeguards in place to ensure the Confidentiality, Integrity and Availability of DJE's ICT resources.
- To monitor the use of DJE's ICT resources to detect and identify any breach of this policy or its related policies.
- To act upon any breach and to bring such breaches to the attention of HR Division.

### 5.3. Responsibilities of Line Managers:

- To comply with this policy in their area of responsibility, including any training and awareness that may be needed for DJE staff, temporary staff, sub-contractors and agency staff.
- To report any breach of this policy and to consult with HR Division on the appropriate subsequent procedures (if any) to be followed.

### 5.4. Responsibilities of Users:

- To read, understand and comply fully with this policy when utilising DJE's ICT resources.
- To comply fully with any instructions issued by ICT Division concerning DJE ICT resources.
- To respect and protect the confidentiality and privacy of the information they are processing at all times.
- To report any breach of this policy of which they become aware.

## 6. Incident Reporting

All users of DJE's ICT resources must immediately contact helpdesk@justice.ie to:

- Report all lost or stolen ICT resources. For portable devices with significant value (for example, laptops, smart phones or tablets) users must additionally report the loss to An Garda Síochána or if abroad to the relevant policing authority.
- Report any actual or suspected breach of information security, including unusual systems behaviour or activity.
- Report the discovery of any vulnerability in any system allowing unauthorised access to information.
- Report any unauthorised interference with ICT resources, including but not limited to altering the hardware or software configuration of a device, removing the device or circumventing any access controls

Where the suspected breach involves personal data, the Data Protection Support and Compliance Office (DSPCO) should be informed immediately by email to dataprotectioncompliance@justice.ie

If you discover material that is potentially illegal,

- You must be careful not to do anything that could be construed as misuse of the material. You must not copy, delete, move, distribute or store such material. You must report the matter to your Head of Division and the Information Security Manager immediately, and you should make a note of events, actions and times, etc. for future reference.
- In all cases where potentially illegal material, or behaviour in breach of this policy is discovered or observed, you must act with discretion at all times, and ensure that information is shared with others on a strictly need-to-know basis.

## 7. Exceptions to Policy

While any non-compliance with policy presents a risk to DJE's desired security posture, it is accepted that exceptions may be required from time to time. All requests for exceptions to the policy must be made in writing to ictsecurity@justice.ie, after which you will be asked to complete a template business case for why you should be allowed an exception.

## 8. Breach of Policy

Breaches will, in the first place, be a matter for Heads of Division in consultation with Human Resources Division, if appropriate. The Head of HR Division will refer any suspected illegal use of DJE's ICT resources to An Garda Síochána.

Where a breach of these guidelines is suspected, the Department will investigate the alleged breach and will take whatever action is needed to allow to secure the network and allow an effective investigation to take place.

The Disciplinary Code, a copy of which is available on the Intranet, will be invoked where necessary. Each case will be considered on its merits and processed in accordance with the Disciplinary Procedures and the principles of natural justice.

Breaches of this policy by a third party supplier/contractor, may lead to the withdrawal of any ICT resources which are made available to that third party and to the possible cancellation of any contract(s) between DJE and that third party.

## 9. Ownership & Review

This policy will managed by the Human Resources Division on behalf of the Department and will be subject to review in consultation with the relevant stakeholders.