

Acceptable Use of Information and Communications Technology Policy

Purpose of this document

This document describes what is acceptable and what is unacceptable use of the company's systems. It has been prepared to help Intu Properties plc employees, agents and third parties understand what they are, and are not, allowed to do using Intu Properties plc systems and services, from both a personal and business point of view. This should be read in conjunction with the Group's Discipline & Capability, Grievance and Dismissal policies.

This document is derived from the full Information Security Policy. Adherence to the Acceptable Use Policy should be sufficient for day-to-day good practice. If you have any doubts regarding acceptable use of company systems, employees must consult their line manager or ICT who can provide clarity.

Scope

This policy applies to all employees, contractors and agents authorised to use information and communication technology (ICT) provided by Intu Properties plc, this includes use of networks, servers, PCs, 'laptops', personal digital assistants (PDAs), Mobile phones (such as Blackberry & iPhone), portable storage devices, tablets computers (such as iPads) and corporate email sessions from a home or cyber café PC. The ICT equipment is provided to enable staff to do their job and to develop an understanding of information and communication technology. Some personal use of equipment and services is accepted, however, this must be considered within the bounds of reasonableness which is explained below.

This document will be updated as the scope of acceptable use policy extends to other platforms and services or where issues of compliance or legislation impinge upon it.

Structure

For each functional area of technology or service supplied by Intu Properties plc, there is a specific set of acceptable, unacceptable and expressly forbidden practice or use.

Acceptable

The activity listed as acceptable defines the degree of flexibility that Intu Properties plc concedes to all authorised users of company equipment. It recognises that the Group wants people to feel comfortable using new technologies and will help in their development in this key area. It also highlights activity by the Group to manage and monitor compliance with the policy.

Acceptable Use of Information and Communications Technology Policy

Unacceptable

This is a definition of what Intu Properties plc believes to be unacceptable use of its equipment and services. Any activity undertaken that falls within this definition could render the user liable to disciplinary action.

Forbidden

These activities are expressly forbidden. Anyone using company equipment for the purposes identified in this category may be committing gross misconduct.

Management access to data

It must **NOT** be assumed that stored information and communication is private: messages can be intercepted or wrongly addressed. All email messages to and from Intu Properties plc employees have their recipients, senders and contents logged. Intu Properties plc Management reserves the right to inspect the contents of any communications or information stored on Group equipment, for the purpose of confirming compliance with policy. Only authorised personnel can access systems in such circumstances and they will guarantee confidentiality except to the extent that is required to follow up breaches, to comply with court orders or to facilitate criminal investigation.

The Group reserve the right to recover the cost of personal use of equipment and will monitor usage and billing detail to identify such use.

ICT support and Internal Audit may occasionally need to undertake activities that fall into 'Unacceptable' category. This is acceptable provided that it is done with the full knowledge and agreement of their Manager and the Chief Information & systems Officer

Intu Properties plc employs monitoring techniques on many of its systems, including email and the Internet access, to enable usage trends to be identified and to prevent unacceptable use. It is clear from information that this delivers that the vast majority of users respect acceptable use.

Acceptable Use of Information and Communications Technology Policy

Glossary

A number of terms are used throughout the Acceptable Use Policy that may need explanation. These terms are defined below to further aid understanding.

Offensive

It is not possible to provide a definitive, prescriptive list of 'offensive' material. However the following identifies the type of material that is 'offensive' for the purposes of the acceptable use policy: "Material that is defamatory, racist or discriminatory on grounds of religion, disability, gender or sexual orientation, or alternatively which is designed to harass, victimise or bully, cause pain or distress to individuals."

Obscene

Literal definitions of obscene describe material that is 'offensive/outrageous or repellent' or material that is 'designed to deprave or corrupt' the audience. For the purpose of this document, any material that will cause extreme offence to a intu Properties plc employee, business partner or visitor will be considered obscene.

Compressed files

Compressed files are ordinary files that have been changed so that they take up less space than the original file. These files when uncompressed can become extremely large and take up large amounts of space on the workstation or server. Commonly used compression tools are widely available and create files with a name extension of .zip.

Executable code

An executable file is one that contains a program, i.e. a particular kind of file that is capable of being executed, that is run, on a computer processor. An executable file usually has a file name extension of .bat, .com, or .exe.

Acceptable Use of Information and Communications Technology Policy

1. Acceptable Use of Telephony

The provision of (voice) telephony by the Group is for business purposes only - whether on a fixed (land) line or on a mobile telephone or device. While the Group reserves the right to recover the costs of personal calls and usage – this is intrusive and expensive and to avoid this, staff are expected to curtail personal use.

Acceptable

- Communication in the course of the Group's business
- Incidental and emergency personal use
- The Group will monitor call charges and usage logs
- The Group reserves the right to recover any costs attributable to personal use

Unacceptable

- Persistent, significant, personal use may become a disciplinary issue.
- Intruding into the working day with personal calls
- Accessing premium rate services
- Allowing non employees to make use of the device
- Ignoring or by-passing security for the device
- Making passwords or PINs available to unauthorised persons

Forbidden

- To conduct business other than the Group's business.
- To disclose confidential information to unauthorised parties
- To use the telephone to communicate anything discriminatory, abusive, obscene, illegal, offensive, potentially libellous or defamatory

Acceptable Use of Information and Communications Technology Policy

2. Acceptable Use of the Internet

Acceptable

- Accessing business related web sites in relation to the user's job
- Accessing web sites (OTHER than those containing pornographic, offensive or obscene material) for non-business related reasons during lunch hours and before or after the working day

Unacceptable

- Spending any period of the working day looking at non-business related Internet sites;
- Tying up large proportions of Internet resources on non-business related activity, to the detriment of genuine business Internet usage. This includes:-
 - Leaving live internet feeds open all day to collect news or sports results;
 - Downloading images, video or audio streams for non-business related purposes;
 - Making repeated attempts to access web sites that, because of their inappropriate content, have been automatically blocked
- Making your password available for other people to use the Internet service on your behalf;
- Using someone else's personal id and password to access the Internet;
- Downloading any copyright material without the owner's permission

Forbidden

- Downloading software used for hacking or cracking passwords.
- Deliberately accessing sites containing pornographic, offensive or obscene material
- Downloading pornographic, offensive or obscene material.

Acceptable Use of Information and Communications Technology Policy

3. Acceptable Use of Email

Acceptable

- Communication in connection with company business
- Occasional personal use during lunch hours and before or after the working day
- Management access to read employees' mail boxes where there is a legitimate business need to do so (e.g. if a person is absent and important email is expected.)

Unacceptable

- Using email for personal, non-business related communication during working hours.
 - Overuse of services for personal, non-business related communication during break times or after hours, e.g. > 5 non-business related e-mail items per day OR
 - Sending non-business related email directly to large distribution groups OR
 - Sending files with attachments (e.g. compressed files, executable code, video streams, audio streams, or graphical images) to internal or external parties
 - Subscribing to non-business related mailing lists

Forbidden

- Sending messages or files through internal email, or via the external mail gateways that contain discriminatory, abusive, pornographic, obscene, illegal, offensive, potentially libellous or defamatory content.
- NOTE: Unsolicited receipt of discriminatory, abusive, pornographic, obscene, illegal, offensive, or defamatory email is clearly not a disciplinary offence, although anyone who receives such material should inform either their manager, an ICT manager or HR immediately.

Acceptable Use of Information and Communications Technology Policy

4. Acceptable Use of servers, PCs, notebook PCs, PDAs, Smartphones, Tablets Devices (including iPADS) and portable storage devices

While the Group reserves the right to recover the costs of personal data usage – this is intrusive and expensive and to avoid this, staff are expected to curtail personal use.

Where possible iPad users should always use Wi-Fi rather than 3G.

Acceptable

- Storing corporate data
- Running company supplied software
- Loading text and images in connection with normal business
- Storing limited amounts of personal data
- Reporting any accidental damage or loss immediately to the ICT Helpdesk

Unacceptable

- Loading unauthorised or untested software, i.e. software not supplied through the formal procurement process by ICT.
- Loading any software without the prior consent of ICT
- Storing corporate data solely on local drives or devices (which are not backed up)
- Making your password(s) available for other people
- Using someone else's personal id and password
- Moving (static) equipment without agreement from the ICT Helpdesk
- Re-allocating equipment to other members of staff other than through the ICT Helpdesk
- Surrender of equipment not in working order, with undue 'wear and tear' or with accessories missing
- Connecting devices (including USB devices - flash storage, cameras etc) to ICT equipment or the network that have not been supplied through the formal procurement process with ICT

Forbidden

- Loading files containing discriminatory, abusive, pornographic, obscene, illegal or offensive content, whether in text, image, video or audio format.
- Physical abuse or wilful neglect of equipment

Acceptable Use of Information and Communications Technology Policy

5. Data & Electronic Information

The management of corporate and customer data and electronic information are increasingly important and we all need to take responsibility to ensure it is appropriately secured and managed. There are significant business impacts and potential legal ramifications if data ends up in the wrong hands. Data may only be sent to internal parties or authorised external parties. Sending such materials to unauthorised parties is strictly forbidden.

Electronic information includes but is not limited to, emails, files, documents, presentations, contracts, PDF's, data extracts, reports, CAD drawings, graphic designs etc.

ICT and Risk & Internal Audit are currently carrying out a more in-depth review of the whole area of data management and further changes will be implemented in due course.

Acceptable

- Accessing data / electronic information to support your day to day work activities
- Providing data / electronic information which is deemed appropriate to your day to day activities to other members of the intu business
- Providing data / electronic information to 3rd parties on a restricted and limited basis if it is required by them to carry out the work for which they are contracted / employed and has been appropriately authorised
- If such data is commercially sensitive or not in the public domain, consideration should be given as to whether the 3rd party should be subjected to a Non-Disclosure Agreement (NDA). If unsure seek advice from your manager or to the Legal department.

Unacceptable

- Sending any data / electronic information within intu that is not part of your role
- Sending confidential data / electronic information outside of acceptable recipients

Forbidden

- Sending data / electronic information to 3rd parties that is not part of your remit of work
- Sending customer / marketing data to 3rd parties which is not in accordance to the Data Protection policy and in line with intu Digital's secure data transfer policy
- Sharing user id's / passwords allowing unauthorised access to systems and data

Acceptable Use of Information and Communications Technology Policy

6. Acceptable Use Policy for the 40 Broadway 'Studio 40' iPads

The Studio 40 iPads are not part of the corporate network and are available for legitimate personal use of the Internet.

Acceptable

- Legitimate personal internet use
- Use of personal (hot) mail account and ISPs. (Take care to log off properly).
- Personal shopping, banking and services - at the user's own risk.
- Available at any time - in your own time
- Use by visitors who accept this section of the policy

Unacceptable

- Use for company (Intu Properties plc) business
- Use of the Studio 40 iPads to the detriment of your working day
- 'Hogging' the Studio 40 iPads at the inconvenience of other staff
- Storing personal information on the Studio 40 iPads

Forbidden

As detailed elsewhere:

- Downloading software used for hacking or cracking passwords.
- Deliberately accessing sites containing pornographic, offensive or obscene material
- Downloading pornographic, offensive or obscene material, whether in text, image, video or audio format.
- Abusive, obscene, discriminatory, illegal, offensive or defamatory messages
- Illegal or illicit trading of any kind.

Acceptable Use of Information
and Communications Technology Policy

7. Acceptable use of Social Media

- **See Social Media Policy**

Date of last review	October 2014
Date of next review	March 2015
Date it was first published	February 2013
Author(s)	ICT & Human Resource Depts
Audience	All employees of the company Contractors Temporary Staff