Get the most out of Glasgowlife™

# Policy on Guidelines and Acceptable use of I.T.

# Acceptable use of our Information and Communications Technology Facilities

## 1. Introduction

This document sets out our policy and guidelines on the permitted use of our Information and Communications Technology (ICT) facilities. It outlines our minimum standard to be followed by all Glasgow Life staff.

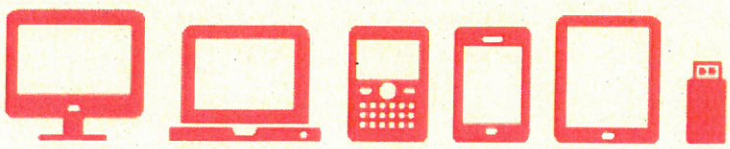
This document (revised September 2015) replaces all previous versions.

## 2. Responsibilities

All users of our ICT facilities are required to read this policy and to comply with it at all times.

If you are a manager or a supervisor you are responsible for:

- ensuring your staff are aware of this policy and have signed a User Access Form before using any of our ICT facilities
- authorising use of ICT facilities in your area
- ensuring your staff comply with this policy when using our ICT facilities
- dealing with breaches of this policy (more information in section nine)
- completing the relevant forms when new staff start, staff move or leave and sending them to Information Services and also Customer and Business Services. This will allow the access rights to our ICT assets to be correctly updated for the member of staff using that asset. For more information on our assets read our Security Guidelines for computer users on the Glasgow Life intranet
- monitoring your staff's use of email and the internet, in line with section 9 of this policy document.



# 3. Policy

We rely heavily on our ICT facilities to conduct our business. Access to our ICT facilities is strictly controlled and monitored. Unauthorised use of our ICT facilities is not permitted - all users must have been authorised by management.

Section 6 and 7 of this policy outline the authorised use of our ICT facilities.

Personal use of our ICT facilities is authorised, but this is at the discretion of your manager, and your use must comply with section five of this policy.

We reserve the right to withdraw your permission for personal use if you breach this policy.

Action may be taken against any individual or group, under our disciplinary code, who do not comply with our guidelines. Details in relation to how non-compliance will be handled can be found in section 10.

For more information you can phone:

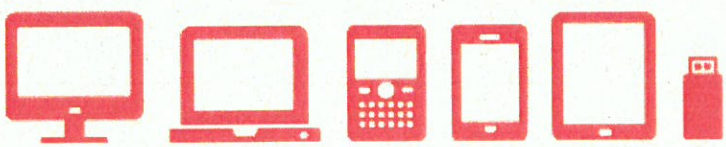
> Glasgow Life HR

> Internal Audit on 0141 287 3777.

# 4. Who It Applies to

This policy applies to everyone who uses our ICT facilities. This includes:

> Glasgow Life staff
> contractors
> consultants
> students
> voluntary workers
> interns
> Modern Apprentices
> Skillseekers



- any other person (except those listed) who have access to our ICT facilities.

This policy does not apply to:

- use of the our internet website by the public
- members of the public using public access PCs in libraries and learning centers
- use of school PCs by pupils.

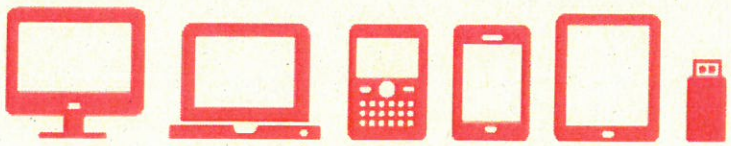
# 5. Working arrangements

This policy applies at all times, to all Glasgow Life working arrangements which includes both offices and agile workers.

This policy applies to all our ICT facilities provided to you to conduct our business. This includes:

- PCs
- telephones (including mobile and landline phones)
- mobile devices (including laptops, Blackberrys®, tablet/hybrid devices, iPads and other Personal Digital Assistants - PDAs)
- USB storage devices (including pen-drives)
- fax machines
- our communications network
- radio systems.

Guidelines on the use of our ICT facilities by Trade Union Representatives can be found in section 7 of this policy.



# 6. Guidelines on personal use of our ICT facilities

Our telephone landlines, or a Glasgow Life mobile phone (including Blackberrys® and smartphones) should not be used for personal use, except in an emergency.

This restriction also applies to the use of a Glasgow Life laptop or tablet which is connected through a mobile phone network or mobile broadband (4G).

However, if you use WiFi or a broadband connection for your device, you are allowed normal personal use as shown in the guidelines below.

You are allowed to use your device for personal use provided it does not:

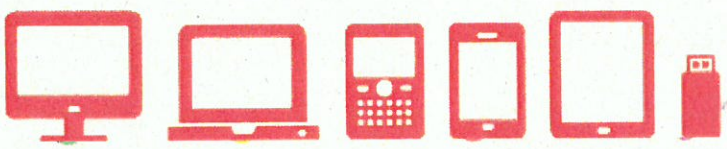
- hinder our business
- incur any additional cost to us
- adversely affect the running of our systems
- bring us in to disrepute.

Personal use can:

- only take place during your own time, unless in exceptional circumstances and it has been approved by your line manager – working areas vary across our Services, make sure you understand your working arrangements
- not breach the general guidelines on use of ICT facilities in section 7
- not make use of business information which has not been made available to the public – access is explicitly prohibited and this would be a criminal offence under the Computer Misuse Act 1990 and the Data Protection Act.

Personal use must not include:

- allowing others, such as friends or family to use your ICT devices
- the storing of personal files, such as music on our ICT devices and network
- accessing social media on a GL mobile device, such as Facebook or Twitter
- using instant messaging such as Skype, Google Talk due to the risk of viruses
- using your business email address to subscribe to mailing lists and clubs
- installing and downloading programs such as games or tool bars
- accessing radio or video content – streaming these places unnecessary strain on our network



- using a 4G or other mobile phone network for personal use of a device
- using file sharing programs
- using encryption to obscure the content of personal messages and files
- the use of web mail services, such as Gmail, unless you are authorised to do so.

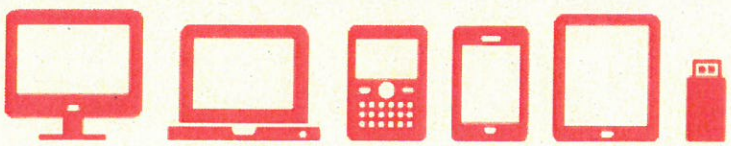
We will not accept responsibility for:

- making backups of personal files
- restoring copies of personal files from backups - as personal storage is not permitted (we reserve the right to delete such files from our system if you have not removed them)
- any financial loss your incur as a result of personal transactions made using our ICT facilities.

# 7. General guidance on the acceptable use of our ICT facilities

These guidelines apply to both business and personal use.

- Software – including media files such as music video, must only be used in accordance with license agreements and UK copyright law. Making, using or distributing unauthorised software copies is illegal, and is not permitted on our ICT facilities.
- Sensitive data – you must follow our Information Security – staff guidelines and Data Protection guidelines on keeping Glasgow Life information secure and your accounts protected. Our guidelines include best practice such as:
  - using encryption for sensitive business data where necessary
  - using a strong password which is not shared with anyone or used on other systems or websites
  - not allowing anyone else to use your IT account
  - not using anyone else's IT account.
- Email – any messages you send from our email systems identifies us as the sender – emails are therefore the same as sending a business letter on headed notepaper. You must make sure that any information you send is appropriate and does not include any personal comments that may conflict with our policies, or bring us into disrepute.



- Mobile Devices – you must take care with the security of any of our ICT facilities, especially mobile devices. Do not leave equipment such as laptops and smart phones in a vehicle – if you have to do this, please lock them securely out of sight, for example in the boot.

You must not use our ICT facilities:

- for illegal activities, including defamation and fraud
- to operate a private business
- to run personal or private software - there is a risk of viruses and to the council network
- for any purpose that would breach our Information Security - Staff Guidelines, Equality Policy, Harassment Policy, Employee Code of Conduct or our Code of Discipline
- to install software or tools that undermine bypass our security systems and policies – this is only permitted by technical staff when authorised by management. This includes any software that would:
  - identify passwords for files and accounts
  - secretly record keyboard input
  - hide the user's identity
  - intercept traffic transmitted across the network
  - enable mass mailing.

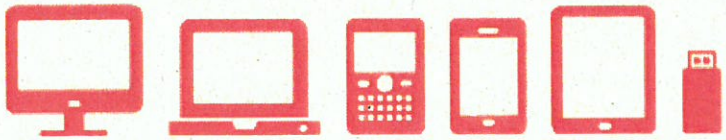
(This above list of examples is not exhaustive).

If you are not sure that your use of our ICT facilities is appropriate please speak to your line manager.

# 8. Guidelines on the use of ICT facilities by recognised Trade Union Representatives

Where ICT facilities are provided as part of the Trade Union facilities , any Trade Union duties, as defined by the Advisory Conciliation and Arbitration Service (ACAS) Code of Practice, will be treated as authorised business use.

Our ICT facilities may not be used for other Trade Union activities (except by agreement of management) or used in conflict with our interests (for example opposition to decisions or ballots for strike action).



# 9. Monitoring of the use of our ICT facilities

Your manager, or supervisor, is responsible for reviewing reports about your use of our ICT facilities. In addition to this, GCC Internal Audit monitor use to make sure that this policy is being applied.

Any breach to this policy will be reported to your Head of Service to deal with.

If you use our ICT systems and facilities you must accept that your usage will be routinely monitored to make sure you are complying with this policy. This monitoring will help to maintain the efficiency and integrity of our ICT systems and includes:

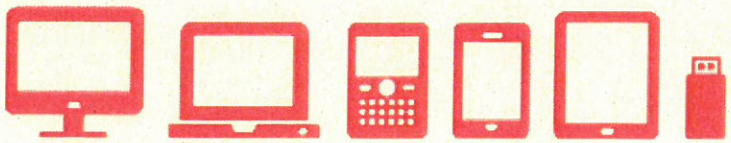
- dialed telephone numbers - the date, time and duration of calls
- the dates, times and addresses of websites visited
- the dates, times, subjects, senders and recipients of emails
- details of all music files stored on our network use of unencrypted USB devices (for example, pen drives)
- details of usage that identifies specific ICT equipment.

We will take reasonable steps to respect your privacy when using our ICT facilities whilst upholding our obligations, as both the service provider, and also your employer, in accordance with our Privacy Statement.

Any managers undertaking monitoring must make sure that they act in a reasonable and fair manner, for example, random spot checks of usage may be legitimate, however extensive monitoring of an entire staff group is unlikely to be.

We may have to conduct detailed investigations, (including accessing the content of files or email messages) for various reasons which can include:-

- making sure our policies, conditions of service, business and security procedures are adhered to
- maintaining the effective operation of our computerised systems
- conducting Glasgow Life business in an employee's absence
- preventing/detecting unauthorised use of communications systems, criminal activities or other serious misconduct



> providing information to individuals or outside agencies, as required by the Data Protection Act1998, the Freedom of Information (Scotland) Act 2002 and/or the Environmental Information (Scotland) Regulations 2004.

Where possible we use automated tools to manage our ICT systems and to protect against inappropriate or malicious material or viruses being passed through our ICT facilities.

Where a trade union representative or member of staff pursuing a grievance is subject to monitoring, this should only be undertaken by the Service or HR team or Internal Audit. This is to avoid any perception that management monitoring is being done to undermine the activities of the union representative or the person raising the grievance.

Managers and supervisors should also avoid opening messages between union representatives and their members for the same reason. If such messages require to be analysed, this should also be done by the Service or HR team or Internal Audit.

# 10. Breaches of this policy or other misuse of ICT facilities

The disciplinary policy will be applied if any individual breaches this policy, or misuses our ICT facilities. Any action taken will be appropriate to the circumstances and may include disciplinary action, up to, and including dismissal.

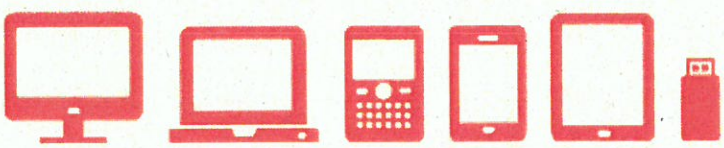
In certain circumstances, breaches of this policy may be reported to the police.

If you are aware of any breach of this policy, you should advise your manager or supervisor, or report the matter to the Head of Internal Audit as soon as possible.

# 11. Employee benefits and resources

We recognise the benefits of this policy (which includes the personal use of ICT facilities as detailed in section 6), as being:

> The enhancement of skills and awareness through responsible and productive use of our ICT facilities
> The assistance in helping you balance your work, lifelong learning and personal life through the use of ICT facilities



> personal use of our ICT facilities is an opportunity to provide a benefit to you at no additional cost to us.

You must complete an annual mandatory course if you use our ICT facilities.

This course is available on our employee development portal called Glasgow Online Learning Development (GOLD) and is called Information Security.

You must complete this course each year so that you are reminded of your responsibilities when using our equipment and how to handle and protect the information you use at work.

In addition to this mandatory course you can also undertake courses to help with your computer skills on GOLD such as:

> Computer Basics
> Webwise.

# 12. Other relevant policies, regulations and codes

For more information please read our:

> Code of Conduct
> Code of Discipline
> Equality Policy
> Information Security Policy
> Security Guidelines for Computer users
> Policy on use of Social Network sites
> Our Privacy Policy and Statement
> Harassment Policy

There are a number of other documents and regulations that are relevant to this policy. These include:

> Computer Misuse Act 1990
> Data Protection Act 1998
> Freedom of Information (Scotland) Act 2002
> Information Commissioner's Employment Practices Code and Supplementary Guidelines.