

**The Atrium Group**

**ICT Controls Policy**

# Approved by Board February 2021ICT Controls Policy

# Introduction

* 1. The purpose of this Information & Communications Technology (ICT) Controls Policy is to ensure the effective protection and proper usage of the ICT systems within The Atrium Group.
	2. This Policy is aimed at anyone using The Atrium Group’s ICT facilities including staff and Board.
	3. The ICT investment of the organisation is considerable, and the dependency on computer technology in the delivery of our housing services is increasingly high. This ICT Controls Policy will assist in maintaining systems at operational level.
	4. Contraventions of the ICT Controls Policy could seriously disrupt the operation of The Atrium Group and any breaches will be treated seriously.
	5. Department Heads are responsible for ensuring adherence to the ICT Controls Policy within their Departments, overseen by the Head of Finance & Corporate Services.
	6. This ICT Controls Policy consists of
* Management of ICT Systems
* Safe & Effective Computer Use
* Acceptable ICT Use
* Unacceptable ICT Use
* Use of Email and Internet

# 2. Management of ICT Systems

## Role of the ICT Officer (System Administrator)

2.1 Although access to certain areas is restricted to certain users, the System Administrator is allowed access to all parts of the system in order for maintenance of the system to take place and for checks to take place to ensure that security is being maintained and e-mail/internet access is not being abused.

The ICT Officer is responsible for the following:

• Develop, implement and review the Information Management and Technology Strategy.

* Co-ordinating ICT support/help desk with external providers

• Business application development

• Web Services and Social Media Development

• ICT Business Services

• ICT Project Management

## Network

2.2 Network management, administration and maintenance within The Atrium Group are the responsibility of the Head of Finance & Corporate Services. Access to and usage of the ICT Systems is restricted to authorised users.

2.3 External consultants are allowed remote access to the server in order to carry out their normal support functions. Any third party seeking access must seek permission through the ICT Officer and the remote session must be monitored.

***Access to ICT Facilities***

* 1. No one may use the ICT facilities without prior registration. Registration to use the Atrium Group ICT facilities constitutes acceptance of this Policy.
	2. Users will be given access to those parts of the ICT system which are appropriate to their role. Unauthorised access to data is not permitted and may result in disciplinary action.
	3. The granting of access rights will be by the provision of user IDs and passwords that enable authorised users to use ICT facilities under the conditions applicable to those facilities. Users must notify the ICT Officer of any changes in their duties or responsibilities which may affect their access and right to use ICT facilities. Any such changes will require approval from their Department Head before being implemented.
	4. Users should ensure that passwords are kept secure at all times. In the event of a user believing a password is no longer secure, this should be changed and notified to the Data Protection Officer (DPO) immediately.

## Hardware (PCs, Laptops, Notebooks, Printer, Modems, Mobiles etc.)

* 1. The requirement for ICT equipment will be identified within the context of the Business Plan, and more specifically within a planned programme of equipment replacement, translated annually into a Budget.
	2. The purchase, installation, configuration and maintenance of all computer equipment is the responsibility of the ICT Officer working with, the Head of Finance & Corporate Services who will maintain computer equipment registers to ensure full tracking of all equipment; and ensure adequate insurance cover for the ICT system. The ICT Officer will ensure all users are aware of any restrictions and limitations on the use of ICT equipment.
	3. Requirements for new hardware should be discussed in advance with the Head of Finance & Corporate Services, to assess the detailed specifications and requirements. The deployment of new equipment or re-deployment of existing equipment is to be undertaken by the ICT Officer, after consultation with Department Heads and the Chief Executive. The relocation of hardware within or out with The Atrium Group premises is not to be undertaken without the permission of the Head of Finance & Corporate Services who will ensure that there is good reason for relocation, determine the most appropriate means of relocation and ensure computer equipment registers and insurance policies are updated.
	4. The security and safekeeping of portable and other equipment used out with The Atrium Group offices is the responsibility of the users using it. Loss of or theft of any piece of equipment must be reported immediately to the Head of Finance & Corporate Services. All portable ICT equipment should be kept securely at The Atrium Group’s offices or at the individual’s home.
	5. All users are responsible for the proper usage, care and cleanliness of the computer equipment they use. Head of Department should ensure that users maintain the cleanliness of their machines.
	6. Problems with hardware should be reported to the ICT Officer in the first instance.
	7. If a user leaves, all equipment should be returned to the ICT Officer and deregistered and re-assigned following direction from the Head of Department.

## Software & Software Applications

* 1. The requirement for ICT software and applications will be identified within the context of the business plan and more specifically within a planned software acquisition and upgrade programme, translated annually into a Budget.
	2. The purchase, installation, configuration and support of **all** software and software applications used within The Atrium Group are the responsibility of the Head of Finance & Corporate Services, who is the custodian of all software used by The Atrium Group. Software, including screensavers, must not be installed or removed by users without prior authorisation from the Head of Finance & Corporate Services: this includes programs and applications downloaded from the Internet.
	3. The Atrium Group will treat the installation and/or use of unlicensed software by users as a serious breach of the ICT Controls Policy. Software licence registers will be maintained by the Head of Finance & Corporate Services to ensure compliance with legislation. Requirements for new software and applications should be discussed in advance with the Head of Finance & Corporate Services to assess the detailed specification and implications.
	4. Problems with software should be reported to the ICT Officer.
	5. Requests for modifications, enhancements and upgrades of existing software applications should be discussed with the Head of Finance & Corporate Services.

## Data, GDPR and Electronic Information

* 1. Data Management is to be in accordance with any data management policies and procedures of The Atrium Group, specifically referring to the Privacy Policy, Fair Processing Notice and Date Retention Guidelines.
	2. Overall responsibility for the maintenance, accuracy and appropriateness of data held lies with the DPO. Heads of Department are responsible for maintaining the quality of the computer-held data processed by their users. The individual user is responsible to their line manager for the quality of the computer data they have personally processed.
	3. All information/data held on The Atrium Group ICT systems is deemed the property of The Atrium Group and must not be accessed or utilised for other than Atrium business. Data may not be disclosed or passed to third parties without the agreement of the relevant Department Head or Chief Executive.
	4. As a condition of employment, users consent to the examination of the use and content of all data/information processed and/or stored by the user on the ICT systems owned and managed by The Atrium Group.

## Back Up

* 1. The Head of Finance & Corporate Services is responsible for ensuring the implementation of an effective back-up strategy for all software and data.
	2. Users of networked desktop or remotely operated PCs and Laptops should not store any data on their local hard drives. Data so stored may be lost if a problem develops with the equipment and it may not be possible to achieve data recovery. This is also against the data protection policies of The Atrium Group. Therefore, all Data should be stored within the file directory (folder) structure used by the office.
	3. No matter how careful The Atrium Group is, no-one can make the system 100% safe and in the event of a disaster which removes data from our ICT systems, we have external back-ups taken daily and stored off site. Restoring these back-ups and the procedures to follow in this instance are detailed in the Business Continuity Strategy & Plan.

## Anti-Virus Protection

* 1. The Head of Finance & Corporate Services is responsible for the implementation of an effective virus security strategy. All machines, networked and standalone, will have up-to-date anti-virus protection. The installation of anti-virus software on all machines is the responsibility of the Head of Finance & Corporate Services who will ensure the upgrade of the anti-virus software on all networked desk-top PCs and Laptops.
	2. Users should not accept any memory stick, CDs, DVDs or other external storage devices from third parties. Users are permitted to use external storage devices for internal transfers only. Should a virus be detected, you should notify the ICT Officer and Head of Finance & Corporate Services, who will provide training and assistance.
	3. Under no circumstances should users attempt to disable or interfere with the virus scanning software or firewalls.

***Working outside of the office***

* 1. The system set up allows for remote access to be obtained from external to the office environment. This can be accessed through an Atrium Group device or a personal device.
	2. All The Atrium Group devices will be pre-set up with the required software for working remotely. Personal devices can down load the software and separate procedures for this are available.
	3. Remote / Home working is to be agreed in advance with Heads of Department.
	4. Staff working remotely must ensure that they take appropriate precautions to preserve the integrity and security of Atrium’s systems. To this end staff working remotely will require to confirm that at all times
* They access on a secure device which is password controlled and private (not a public one).
* They use a secure private Broadband connection which is not shared or public
* Work takes place in a secure and private location
* The work area and equipment set up is DSE compliant and you can work comfortably at a desk or table.
* They are mindful of GDPR considerations and always ensure that
	+ Their screen and any work related materials are not visible to anyone other than themselves
	+ any conversations with customers and colleagues are private and cannot be overheard by others
	+ confidential materials are not left where they could be seen by others
* They can communicate easily using Horizon software with colleagues (via video and phone)  and customers (via phone)
	1. These precautions are indicative. Staff members who breach the integrity or security of the system either by their actions or inactions, may be subject to disciplinary action.

## Safe & Effective Computer Use

## Health & Safety

* 1. Health and safety with regards to The Atrium Group computer equipment and computer work stations will be managed to comply with Health & Safety legislation, policies and procedures.
	2. The Health and Safety Administrator will ensure that computer users are advised on the safe use of equipment and that risk assessments are conducted as necessary. Users requiring additional equipment to facilitate safe usage should contact the Head of Finance & Corporate Services.
	3. Heads of Department are responsible for ensuring health & safety legislation and procedures with regards to computer equipment are implemented within their Departments.
	4. The Head of Finance & Corporate Services will keep abreast of IT-related legislation and advise accordingly.

## Training

* 1. It is the responsibility of Head of Departments to ensure appropriate computer training for their users is identified and undertaken. The Head of Finance &Corporate Services will advise on computer-related training issues.
	2. Staff will be provided with training on procedures and processes for using the main systems and will be expected to adhere to those procedures and processes. Staff who wilfully and consistently deviate from procedures and processes, thus compromising our systems, may be subject to further action.
	3. All staff will be expected to demonstrate a basic level of ICT literacy across the systems which Atrium uses. The appropriate level of ICT literacy may vary from post to post but will be developed by Department Heads for their staff.
	4. ICT competency testing will be done periodically to establish training needs. Staff members who, after appropriate training, are still unable to demonstrate an appropriate level of competency, may be subject to further action.

## User Accounts

* 1. Heads of Department should notify the Head of Finance & Corporate Services of new users and/or roles in advance to allow the creation of network and e-mail accounts and system permissions.
	2. Heads of Department should notify the ICT Officer of the departure of users and/or changes in roles to allow the deletion of network and e-mail accounts.

## User IDs & Passwords

* 1. The Head of Finance & Corporate Services is responsible for the implementation of all The Atrium Group ICT security measures.
	2. Users will be provided with a unique user-name (user ID) which they will require to use in conjunction with a password to access the system.
	3. Users are responsible for the security of their password which they should not divulge, even to colleagues.
	4. Users should change their passwords when prompted by the system in the case of networked machines or on a regular basis for standalone machines.
	5. Passwords should be made up of at least 8 characters, and contain a mixture of upper and lower case letters, numbers and special characters.
	6. Problems with ICT passwords should be reported to the ICT Officer and Head of Finance & Corporate Services.

## ICT System Usage

* 1. Users should ensure their computers are fully shut down and turned off at end of day.
	2. Computers should not be left open whilst the user is absent. Users should log out, lock or shut down the computer if leaving it unattended.

***File Management***

* 1. Department Heads will determine the top-level folders/directories and associated permissions required for the efficient running of their department, and inform the Head of Finance & Corporate Services accordingly.
	2. The Head of Finance & Corporate Services is responsible for setting up, and managing, the overall top-level file structure for The Atrium Group.
	3. Within their respective top-level folders, users should create sub-folders in accordance with their own departmental guidelines but cannot create new top-level folders.
1. **Acceptable Use of ICT Systems**
	1. The Atrium Group believes it is important that users have a clear understanding of the expectations that the Company places on them, and the standards to which they are expected to work. This includes the way in which they conduct themselves at work.
	2. The significant growth in the use of ICT in the workplace has led to the development of new working practices for many users. Future technological developments are likely to further influence and change the workplace and will require users to continue to demonstrate a positive and flexible response.
	3. This section outlines the expectations and requirements placed on users in relation to their use of The Atrium Group's ICT systems in the workplace and where appropriate elsewhere.

***Approach and Scope***

* 1. The underlying philosophy is that the ICT facilities provided by The Atrium Group should be used in a manner which is ethical, legal, and appropriate to the Company’s aims and objectives.
	2. ICT facilities includes all computer and computer-based systems and/or computing hardware, software and connectivity (both internal and external) made available by the Company irrespective of their location at the time of use.
	3. Users of The Atrium Group ICT facilities are expected to comply with the conditions of use, which include the following. Users must not:
* Disclose user IDs and/or personal passwords which give access to the system
* Enable unauthorised third party access to the system
* Delete, amend or otherwise corrupt the data managed and inserted by other users
* Knowingly introduce viruses or other harmful programmes or files
* Attempt to gain deliberate unauthorised access to external facilities or services
* Use The Atrium Group ICT facilities to send unsolicited, unauthorised commercial or illegal advertising or other material
* Load software for which no licence is held
* Modify software
* Use The Atrium Group ICT facilities for commercial gain out with the requirements of The Atrium Group
	1. The General Data Protection Regulations outline the legal position in relation to the use of data. Users requiring advice about the content or implications of this Act should contact the Head of Finance & Corporate Services, who is the Atrium Group Data Protection Officer.

***Social Media Platforms***

* 1. The Atrium Group respects the right to a private life and that includes joining any social medial platforms employees wish. However, information posted on such sites is classed as public and not private. Employees are therefore not allowed to disclose confidential information relating to the Group, its customers, partners, suppliers, Board members, or any other stakeholder on any social networking platform. It is also prohibited to post any comments on people and events connected to The Atrium Group, or make any remarks that could potentially bring the Group into disrepute.
	2. If using social medial platforms employees are expected to adhere to the following:
* Keep profiles set to private and protect tweets,
* Ensure all passwords are kept private,
* We do not prohibit employees from listing The Atrium Group as their employer however we do advise against it,
* Employees should be aware of the language and content of their posts,
* We would recommend that users do not associate themselves with either Atrium Homes’ or Choice Places’ Facebook pages by friending or choosing to “like” any of the content.
1. **Unacceptable Use of ICT Systems**
	1. Unacceptable use of or behaviour in relation to the use of The Atrium Group ICT systems will not be tolerated. Any alleged inappropriate or unacceptable use of the ICT facilities will be investigated, and may be the subject of disciplinary action where necessary.
	2. The following behaviour will always be considered to fall below the standard of acceptability:
* The creation, display, downloading, production, circulation, storage or transmission in any form or medium of pornographic or other offensive or illegal material from any source
* Forwarding confidential, sensitive or personal information to 3rd parties or any other unauthorised recipient.
* Using the ICT system for personal commercial gain
* Accessing social media or similar sites during normal working hours.

***Copyright and Licensing***

* 1. Users have a responsibility to ensure that copyright and licensing laws are not breached when composing or forwarding Emails, Email attachments and using the Internet. The laws regarding breach of copyright apply equally to the downloading and copying of information from the Internet: users must be clear whether or not there is an entitlement to download the required information.

***Excessive Personal Use of the ICT System***

* 1. The prime purpose of providing access to the Atrium Group ICT system is to enable users to fulfil the responsibilities of their role. It is recognised that users may need to conduct private business during office hours; however, excessive personal use of the ICT facilities is not acceptable.
	2. Personal use is also expected to be limited, where possible, to non-work hours i.e. before and after work and during lunch periods.
	3. Users utilising the system to produce personal printed material should be aware of the direct costs to The Atrium Group. Extensive proposed use should be brought to the attention of the Head of Finance & Corporate Services in advance and may be recharged to the users concerned.
1. **The Use of Email**
	1. The Atrium Group recognises the value of Email as an important means of communication. Therefore, it is important that all users recognise that there are also limitations to its use.
	2. Users are referred to section 6.7 of this Policy which explains more about the protocols relating to email usage.
	3. Users are to pay the same care and attention to the composition of Email messages as to the other forms of written communication. An informal communication may be appropriate in some circumstances, for example internal message exchanged by office colleagues. It will not however be appropriate when an issue is more formal, or when communicating externally. Email can lack the context, cues and clues that convey the sense of the message, and the wrong impression can easily be conveyed. Email is a form of publication governed by the rules of disclosure, libel and employment law.
	4. We recommend that users set up folders within their email and file messages accordingly. This is in order to maximise efficiency of the system.
	5. Confidential material sent by e-mail should be so marked but sent only with caution.
	6. The Atrium Group retains the right to access and view all Emails sent and received by the Email system. This right is exercised solely through the Head of Finance & Corporate Services.

***Appropriate Vs Unacceptable Use of Email***

* 1. The use of Email is unlikely to be appropriate when:
* The information to be communicated is complex and/or lengthy
* The recording of discussions about a topic is necessary
* A signature is required on a communication
* The communication includes information of a sensitive, personal or confidential nature
* Storage or retention of information is required
	1. Even though in a particular situation email may be an appropriate medium of communication, the content of the email itself must be controlled. When using E-mail users must also be aware of aspects of use which are unacceptable. The following behaviour will always be considered to fall below the standard of acceptability:
* The use of inappropriate language in communications
* Sending messages which are discriminatory, sexually harassing or offensive to others on the grounds of age, race, disability, gender, gender reassignment, religion or sexual orientation
* Sending messages which could bring the organisation into disrepute
* Sending defamatory messages which criticise other individuals or organisations
* The creation, display, downloading, production, circulation, storage or transmission in any form or medium of pornographic or other offensive or illegal material from any source
* Forwarding confidential, sensitive or personal information to 3rd parties or any other unauthorised recipient.
* Using the ICT system for personal commercial gain
* Sending messages which are rude, overbearing, aggressive or bullying.
* Accessing social networking, dating or similar sites
	1. The Atrium Group e-mail system is a core business application. It should not be used for political, business or commercial purposes not related to The Atrium Group
	2. The Atrium Group e-mail system must not be used to send illegal or inappropriate material.
	3. It is a condition of employment that all users consent to the examination of the use and content of their email accounts as required.
	4. Global distribution lists should be used appropriately. Email to all users (spamming) should be used only when appropriate.

## The Use of the Internet

* 1. Access to the Internet is provided for business purposes. Limited personal use is permitted and is to be restricted to lunch breaks and periods out with working time.
	2. Users must not make inappropriate use of their access to the Internet and must not subscribe to chat rooms, social networking sites, dating agencies, messaging services or other on-line subscription Internet sites.
	3. Programs, including screensavers, must not be downloaded from the Internet without authorisation from the Head of Finance & Corporate Services.
	4. The Atrium Group retains the right to monitor Internet usage by users. This right is exercised solely through the Head of Finance & Corporate Services. It is a condition of employment that all users consent to the examination of the use and content of their Internet activity as required. Abuse of Internet access may lead to removal of the privilege of access from an individual’s workstation or, in some cases, disciplinary action.
1. **Source of Advice and Assistance**
	1. Any queries about this policy should be directed to the Head of Finance & Corporate Services.

# Contravention of the IT Policy

* 1. Users are to be aware of their responsibilities under the General Data Protection Regulation (GDPR) (2018), Computer Misuse Act and the Copyright Design and Patents Act. The Head of Finance & Corporate Services will provide guidance where required.
	2. Contravention of the Atrium Group ICT Policy or any act of deliberate sabotage to The Atrium Group ICT systems may be considered a disciplinary offence and could result in disciplinary action, including dismissal.
1. **Review**
	1. This policy will be subject to regular review or in response to changing ICT provision within the organisation or legislative or other sectoral changes.