Cernach

Information Security policy

Approved by Management Committee:	August 2021
Latest review date:	August 2024

Information security policy

1. Introduction

1.1 The Association has invested considerably in the use of information and communication technology (ICT). In many areas of our work now the use of ICT is vital and must therefore be protected from any form of disruption or loss of service. It is therefore essential that the availability, integrity and confidentiality of the IT systems and data be maintained.

1.2 This policy complements the ICT asset replacement plan.

2. Policy objectives

2.1 There are four main objectives of this policy in relation to information security.

a) To ensure business continuity and minimise business damage by preventing and minimising the impact of security incidents
b) To ensure that all of the Association’s assets are adequately protected on a cost-effective basis against any action that could adversely affect the ICT services required to conduct our business
c) To ensure that staff are aware of and fully comply with all relevant legislation and
d) To create and maintain within all sections a level of awareness of the need for ICT security to be an integral part of our day-to-day operation so that all staff understand the need for ICT security and their own responsibilities.

2.2 The purpose of this policy is to ensure that:

a) All information, be it stored on computer (including remote access devices such as iPads), transmitted across the network, printed out or written on paper, sent by fax, stored on tapes and discs/within a cloud, or spoken in conversations and over the telephone, is protected against unauthorised access, disclosure, modification or interruption.
b) Confidentiality of information will be assured.
c) The integrity of information will be maintained.
d) Regulatory and legislative requirements will be met.

e) Business continuity plans will be produced, maintained and tested.

f) All breaches of information security, actual or suspected, will be reported to and investigated by the Data Protection Officer (at the time of writing, this is outsourced and the relationship managed by the Corporate Services Officer).

3. Risk management

3.1. The Association has considered the risks involved in purchasing, operating and maintaining ICT and office equipment. An ICT Strategy was established to monitor effectiveness of ICT software and hardware along with a prudent approach to hardware replacement. In addition, the Association shall take cognisance of the General Data Protection Regulation (GDPR) 2018 when storing data.

3.2 Similarly, we have an asset replacement plan was introduced whereby purchase of office furniture and equipment is monitored on a quarterly basis, with the plan being reviewed on an annual basis to inform the budget process.

3.3 All staff are required to be involved in the review process of the information security policy and receive an update of the policy. This ensures all staff are fully conversant with their requirements when dealing with and storing/retrieving information.

3.4 To help ensure that the Association is adequately managing any risks associated with data protection, we will ensure that this area is included in the internal audit programme once every five years, or more often if required or indicated by our independent internal auditors.

4. Equality and human rights

4.1 The Association's equality and human rights Diversity policy, which was approved by the Committee in April 2021, outlines our commitment to promote a zero tolerance to unfair treatment or discrimination to any person or group of persons, particularly on the basis of any of the protected characteristics[1]. This includes ensuring that everyone has equal access to information and services and, to this end, the Association will make available a copy of this document in a range of alternative formats including large print, translated into another language or by data transferred to voice

4.2 We are also aware of the potential for policies to inadvertently discriminate against an individual or group of individuals. To help tackle this and ensure that it does not occur, best practice suggests that organisations carry out equality impact assessments to help identify any part of a policy that may be discriminatory so that this can be addressed (please see section 6 of the equality and human rights policy for more information).

4.3 In line with the Equality and Human Rights Commission screening tool, an impact assessment is not required for this policy.

5. Responsibilities for security

5.1 The Director and Housing Services Manager are responsible for the computer equipment under their control and for its proper use. ICT security is the responsibility of all members of staff.

5.2 The information security policy will apply to all staff and it is the responsibility of each individual staff member to adhere to it.

5.3 All providers of ICT services must ensure the security, integrity and availability of data within the service provided.

6. Legislative and regulatory frameworks

6.1 The Association has to seek to abide with all legislation affecting ICT. All employees and agents of the Association must comply with the undernoted Acts and may be held personally responsible for any breach of

[1] The Equality Act 2010 identifies the "protected characteristics" as age, disability, marriage and civil partnership, race, religion or belief, sex, gender reassignment and sexual orientation.

current legislation listed below and any future legislation that may be enacted.

a) General Data Protection Regulation (GDPR)
b) Copyright Designs and Patents Act
c) Computer Misuse Act

6.2 Standards have been produced to support the policy. These include virus control and passwords and described in section 8.

6.3 Standard 4.3 of the Scottish Housing Regulator's Regulatory Framework states "The governing body identifies risks that might prevent it from achieving the RSL's purpose and has effective strategies and systems for risk management and mitigation, internal control and audit." The purpose of the information security policy is to help ensure relevant parties understand their own and the Association's role in data collection and that this is controlled within these principles.

7. Standards and procedures

7.1 Physical access

7.1.1 Precautions should be taken to ensure that access to PCs is restricted at all times to authorised personnel.

7.1.2 Equipment should be sited to reduce the risk of damage, interference and unauthorised access.

7.2 Software access

7.2.1 Passwords specific to individual staff members will be used to access data on PCs and the server. Adequate mechanisms should exist to ensure access to a PC by authorised personnel can always be achieved. Terminals should not normally be left 'logged in' when unattended.

7.2.2 Passwords will be used to protect all systems and should not be written down or disclosed to others.

7.2.3 All staff will be given a password for specific access to certain systems. For example:

a) Computer server files (full or restricted, depending on role)
b) SDM database (as appropriate to their role)
c) Kelio flexi system (CSO administrator access/line managers approvers and all staff standard access)
d) Allpay (HSM, SHO, HCSO, HOs, AHOs, HA & FO)
e) GCC's HARP grant administration system (D and FO administrator access/ HSM, SHO, SMO access in line with their roles)
f) GCC's e-landlord database (housing management staff only)

7.2.4 Passwords should comprise a minimum of six alphanumeric characters arranged in such a way as they will not be easily guessed.

7.2.5 All staff will be prompted every 90 days to change their password to a previously unused password. These passwords must be provided to the ICT support provider (currently Brightridge) who will store them confidentially; in an emergency, the Director (or most senior member of staff available in the Director's absence) may contact the ICT provider to *break in* to the pc if access is needed. This will result in the staff member having to reset their password on their return to work.

7.2.6 Employees will be held liable for any misuse of a computer resulting from misuse of their password and/or username.

7.2.7 The password given will limit access according to job role. Some users will be given 'read only access' to certain information or programmes and be denied access to others. This is consistent with good practice in relation to the GDPR and information security precautions to ensure business continuity by preventing and minimising the risk of security incidents and/or accidental loss or destruction to data.

7.3 Unauthorised access to physical or electronic information

7.3.1 The Association as a whole, and individual members of staff in particular, will take all reasonable steps to ensure that no one is able to access information that is sensitive/confidential. An example of this would be staff files (both hard copy and electronic).

7.3.2 The circumstances surrounding any unauthorised access to information will be considered and any weaknesses in controls will be explored with the person responsible to the information.

7.3.3 However, it is important for all staff to recognise that, whilst the “keeper” of the information has a responsibility to implement appropriate safeguards to prevent any unauthorised access, everyone else has a duty not to access information unless they have a right to do so. Anyone seeking to access files without a right to do so may leave themselves open to further action, including disciplinary action.

7.4 Information

7.4.1 Information held on the Association’s ICT files or printed format is the property of the Association and is governed by the provisions of the GDPR.

7.4.2 Information held should only be released to authorised persons and ICT facilities must only be used for authorised purposes.

7.4.3 Where authorisation is given for personal work, this activity must be undertaken in the staff member’s own time, and must not interfere in any way with the Association’s ICT service provision.

7.5 Virus protection

7.5.1 All PCs, including the Association’s laptops, are protected by virus detection software Webroot AV.

7.5.2 The Corporate Services Officer, in liaison with the ICT support providers, will ensure the virus protection software is updated regularly to guard against new viruses. This is to be included within the ‘health checks’ carried out by the ICT contractor. Webroot is automatically updated with latest threats and viruses to ensure fully updated and all times.

7.5.3 Any detected viruses must be reported to the Corporate Service Officer (or, in their absence, a senior member of staff) immediately.

7.5.4 This virus detection software should not be turned off or disabled.

7.5.5 All staff must ensure the ‘preview’ pane in their inbox is switched off. This will minimise the risk of inadvertently opening an ‘infected’ message.

7.5.6 All staff are required to take care when receiving messages. If uncertain about source of message or if it is clearly ‘spam’, the message should be moved to the ‘junk box’.

7.6 Software copyright

7.6.1 The copying of software programmes for which the Association holds a licence is prohibited and is an offence. Such action could lead to a large fine or imprisonment.

7.6.2 All system discs and licences are recorded and filed by the Corporate Services Officer. It is not permissible to install or insert any software not licensed to the Association. This includes screen savers, games and free software from magazines.

7.6.3 Personal software must not be loaded onto the Association’s computers under any circumstances. If the software is deemed to be of use to the Association, then it should be duly acquired under licence.

7.6.4 Deliberate unauthorised access to copying, alteration, or interference with computer programmes or data is prohibited.

7.6.5 Internal in-house audits will be conducted by the Corporate Services Officer, with assistance from the ICT support provider, to ensure compliance with these provisions.

7.7 Computer misuse

7.7.1 All staff wll be made aware of their access rights for any given hardware, software or data and should not experiment or attempt to access hardware, software of data for which they have no approval and/or need to conduct their duties.

7.6.2 The downloading of any material that is:

- Offensive
- Pornographic
- Profane
- Discriminatory
- Contrary to the principles of the Association's equality and human rights policy

is strictly prohibited and may, in some cases, also be illegal. If a member of staff is in any doubt about whether material fits into this category, then the member of staff should err on the side of caution. Any breach of this requirement could result in disciplinary procedures being invoked and, where it is considered appropriate, we may involve our legal advisors or the Police.

7.7 Business continuity planning

7.7.1 All of the Association's computers are connected to the network therefore the prime copy of all data must be held on the network file server and not the local hard drive. Back-up includes Microsoft Outlook files and SDM and covers both terminal and exchange server data.

7.7.2 All relevant staff (for example the Director, management team, Corporate Services Officer or Finance Officer) should make provision for the safe storage and retention of important records – for example ledgers, vouchers, invoices, staff records, salary details, tender register, former tenant records).

7.7.3 In the event of a complete loss of the ICT systems due to failure of the server through fire, flooding of breakdown the Association should in the first instance contact the appropriate soft/hardware maintenance contractor (details contained within Disaster Recovery Plan). The cloud server can be enabled to allow staff to work from anywhere via a secure

VPN, the ICT provider will then obtain new hardware and rebuild the servers from the cloud back up the system continues to update and back up additional work).

7.7.4 In the event of more serious disasters the Association's disaster recovery plan should be followed.

7.8 The internet and electronic mail

7.8.1 Occasional and incidental social communications using any communication tools are not disallowed by this policy and are permitted so long as this does not interfere with employees' performance of their expected duties.

7.8.2 By using the Association's email all staff expressly waives any right of privacy in anything he or she creates, stores, sends or receives.

7.8.3 During the induction process, staff are given an explanation about the information security policy and all staff are advised of subsequent reviews.

7.8.4 The Association is committed to working towards a paper free environment and staff are requested to store emails received and sent in the relevant folder on the server or Outlook. Where this is not possible or indeed, appropriate, staff are required to print a copy of the email and insert in the proper file.

7.8.5 Staff should avoid sending confidential information via email and should be mindful of the risks of transmitting confidential personal information by email. An automatic disclaimer is added to email messages prohibiting transmission of the message to anyone other than the recipient.

7.8.6 The same care should be extended to email messages as with any form of communication used by the staff.

7.8.7 Viruses are introduced to your PC via email attachments or by using 'infected' discs. Do not insert any discs unless authorised to do so and do not download files or open attachments unless authorised to do so and/or they have been virus checked. Users should take care not to infringe copyright when downloading material or forwarding it to others.

7.8.8 Contact the ICT support provider immediately if you suspect your PC may be infected and cease usage until checked.

7.9 General 'house-keeping' rules

7.9.1 In order to maintain an efficient system, all staff are encouraged to address the following at least on a weekly basis:

a) Delete the 'junk mailbox'
b) Delete the 'sent items'
c) Delete the 'deleted items'
d) Ensure messages retained in the 'inbox' are required and if not, delete them or file them in Outlook files or onto the server.

7.9.2 Harassment (cyber bullying) via any communication tool is prohibited.

7.9.3 Should staff receive inappropriate messages, they are aware of their right to raise concerns with their line manager and that this should be done immediately.

7.9.4 Staff also have the right to raise a grievance should they receive offensive messages or be concerned over a colleague's general use of the internet/ email resources.

7.9.5 Staff are reminded that they should never send messages in anger. This could be in response to a criticism of themselves or the organisation, however, staff should take a few moments to consider the reply and avoid saying something that would be regretted.

7.9.6 The Association does not operate a *postmaster* system. Therefore, messages which are deemed as undeliverable by the System Administrator shall be returned to the originator with a reason for delivery failure. All staff are aware of their requirement to deal with the reason for delivery failure appropriately.

7.9.7 When staff are away from the office for one day or more, they shall set up the ‘out of office assistant’. This will clearly state the period of absence and who to contact should an emergency arise.

7.10 Protection of hardware/physical security

7.10.1 Staff should take particular care when eating and drinking near computers as spilling liquids on the keyboard can be particularly damaging.

7.10.2 Portable equipment such as the Association’s laptop computers, digital camera, overhead projectors should not be taken off site without permission. Staff transporting such equipment should check that they are insured to carry equipment in their car.

7.11 Remote/home working

7.11.1 Home working became the norm during large parts of the Covid-19 pandemic and there are also instances where information may be removed from the office and taken to another site.

7.11.2 Rather than be prescriptive in this regard, we would ask staff to ensure that all reasonable steps are taken to protect any information if it is removed from the Association’s premises. This is particularly important where the information is personal and/or sensitive.

7.11.3 In the event that there is a breach or loss of information, then the staff member must contact the Director (or, in their absence, another senior member of staff). It is important that we can take steps to limit the damage and, following on, ensure that similar instances do not recur.

8. Policy review

8.1 The information security policy will be reviewed every three years, or earlier in line with legal, regulatory or best practice requirements. The next review is therefore due in or before August 2024.

Employee declaration

I am fully aware of and understand the Association’s information security policy (as approved by the Management Committee on 5 August 2021) and I agree to adhere to it at all times. By signing this declaration, I expressly waive any right of privacy in anything I create, store, send or receive using the Association’s computer equipment for internet, email access and other general use.

Name	Designation	Signature	Date
Jordan Allan	Assistant Housing Officer		
Paula Baylis	Housing Services Manager		
Tony Birmingham	Assistant Housing Officer		
Kirsty Boag	Housing Services Assistant		
Karen Dyson	Finance Officer		
Ruth Ghumman	Housing Assistant		
Caroline Jardine	Director		
Holly Lochran	Senior Maintenance Officer		
Siobhan Mangan	Corporate Services Assistant		
Carylanne McLellan	Assistant Maintenance Officer		
Emma McShane	Hsg & Corp Services Officer		
Jim O’Connor	Housing Officer		
Andy Parker	Welfare Rights & TS Officer		
Laura-Jane Richards	Senior Housing Officer		
Ted Scanlon	Community Connector		
Anne Smith	Corporate Services Officer		
Bruce Strathearn	Maintenance Officer		