SPIREVIEW
HOUSING ASSOCIATION

IT System Security Policy

AS WITH ALL OF THE ASSOCIATION'S POLICIES & PROCEDURES, THIS DOCUMENT, IN FULL AND IN PART, IS AVAILABLE IN SUMMARY, ON TAPE, IN BRAILLE, AND IN TRANSLATION INTO MOST OTHER LANGUAGES.

PLEASE ASK A MEMBER OF STAFF IF YOU WOULD LIKE
A VERSION IN A DIFFERENT FORMAT

Date Approved: **January 2025**

Next Review Date: **January 2028**

CONTENT

IT SYSTEM SECURITY POLICY

INTRODUCTION

1. This policy describes our arrangements for ensuring, so far as is possible, the security of our computer systems, which we regard as an essential part of the efficient and effective provision of our services.

2. The policy applies to all Spire View Housing AssociationAssociation:

   - Staff

     and where applicable -

   - Management Committee Members;
   - Contractors;
   - Volunteers;
   - Agents; and
   - any others who use, or are given access to, the communications equipment and computer systems provided by us.

   All who have access to the Association's IT system are referred to in the remainder of this policy as 'users'.

3. This policy covers the use of all items which can be described as IT equipment or systems, including communications equipment, which are provided by the Association to authorised users.

SECURITY OF IT EQUIPMENT & SYSTEMS - GENERAL PRINCIPLES

4. We will implement the following measures to ensure, so far as is possible, the security and integrity of our IT systems and equipment:

5. Users will not be allowed access to any IT equipment or systems until they have:

   - read this policy and confirmed their agreement in writing (by email or by signing a copy of this policy) to comply with its requirements; and
   - received the required initial induction training on the system from our IT support provider and/or the relevant line manager.

6. Access to the IT system will be via confidential personal password and username. Users will be required to change their password at regular

intervals, as initiated by our IT system.

7. Users must not leave their computer screen unlocked when they are away from their desk. All screens must be locked, or the staff member must sign off the IT system.

8. Users will only have access to those parts of the system that they need to use to carry out their duties, and they will not attempt to access areas of the Association's IT network they are not authorised to access.

9. Users will not transfer material from external CD/DVD's or USB drives without the approval of a member of the Senior Management Team. and must not connect any personal device to our computers.

10. All software will be purchased by the Association from recognised, approved suppliers and will be checked and authorised for use by our IT Support provider before it is installed.

11. All staff have access to their own 'One Drive' on Microsoft Office 365, which can be used to store personal data. Please refer to 'Personal Use of IT System' below for more information.

12. Computer data will be regularly saved and backed up.

13. Comprehensive anti-virus software and firewalls etc. will be installed and kept up to date, to protect computer systems. Appropriate maintenance contracts and system support arrangements will be entered into and updated regularly as required.

PERSONAL USE OF IT SYSTEM

14. Users may use their computer and any communications equipment and systems provided by the Association for personal purposes, so long as:

    - all personal use complies with this policy and is lawful;
    - personal use is always undertaken during a user's lunch break or out-with working hours;
    - in the case of Association mobile phones, the combined business and personal use must <u>not</u> exceed the monthly allowance for that phone and incur additional costs through 'non-business' use (for example through the use of premium rate phone numbers). Except in very exceptional circumstances, the use of our mobile phones for personal use must be restricted to the user's lunch break or out-with working hours.

15. Failure to comply with the principles above will be a breach of this policy and will be dealt with accordingly. Where additional costs are incurred through 'non-business' use these will be charged to the staff member concerned.

TRAINING

16. All new users will receive the necessary training before they are permitted to use our computer systems and any other communication systems or equipment - plus on-going refresher training as required e.g. when new software is installed, or systems are upgraded.

17. Specific training will be provided to meet individual user's development needs, e.g. as identified as part of the annual staff appraisal.

18. Training will emphasise that any breach of the current law relating to the use of computer systems, or any breach of this policy, will be regarded as a serious offence which will be dealt with in accordance with our Code of Conduct / Disciplinary Policy (for staff) or the Code of Governance (for Committee Members).

19. All staff must undertake regular Human Risk Management (e.g. USecure) training provided.

20. Breaches by other users e.g. Contractors or Consultants etc. will be dealt with in accordance with the terms of their contract or appointment.

Temporary staff etc.

21. When required, the relevant line manager will ensure that the competency of any temporary, volunteer, freelance or consultancy staff is confirmed before they are allowed access to our computer and other communications systems.

MONITORING

22. The Director will approve appropriate arrangements to monitor the use of the Association's computer systems, to:

- ensure compliance with current law, this policy and the supporting procedures;
- ensure standards of service are maintained;
- provide evidence of transactions and communications;
- help combat unauthorised use of our communications equipment and systems and maintain security; and
- better understand our requirements in terms of the provision of

communications equipment and systems.

23. All monitoring of communications will be carried out in accordance with the requirements of the Data Protection Act 2018 which outlines General Data Protection Regulations (GDPR).

24. Monitoring records may be used as evidence in any action that may result from possible misuse or abuse of our systems or this policy.

Privacy

25. As part of initial and on-going training, users will be advised and reminded that they should not expect any privacy in their use of the Association's computer and communication systems, **even when** they are using the systems for authorised private work in their own time. By using the Association's communications equipment and systems for personal use, users will be regarded as having consented to any personal communications being logged and monitored as described above.

EMAILS & TEXTS

26. Users are reminded that emails or texts sent on behalf of the Association have the same legal authority as signed letters on headed paper, and they are admissible as evidence in a court of law. Users can therefore be held to account for all expressions of fact, intention or opinion made via email or text, - in the same way as with verbal or written statements. Users are also reminded that emails that have been deleted from the system can be traced and retrieved, and the originator can be identified.

27. Users will ensure, so far as is possible, that they are aware of what constitutes confidential or restricted information (e.g. personal and/or sensitive data) and that they do not breach confidentiality or GDPR when sending emails or texts without specific permission.

28. Information sent should be that which can be read by the intended recipients without causing commercial damage or breaches of data protection.

29. When required, confidential and restricted information that is permissible to send should be attached to an email with appropriate encryption or password protection. If a password is used, this should be sent to the recipient in a separate email.

30. Users must ensure that they do not break current laws covering the use of computer systems and electronic communications, including the:

- Malicious Communications Act 1988 (as amended by Section 43 of the Criminal Justice & Police Act 2001):
  The Malicious Communications Act 1988 (MCA) is a British Act of Parliament that makes it illegal to "send or deliver letters or other articles for the purpose of causing distress or anxiety". It also applies to electronic communications.

Computer Misuse Act (CMA) 1990

Current Penalties & Amendments
While the text is broadly correct, you may wish to expand or clarify the penalties to reflect both summary and indictment proceedings in Scotland.

1. **Unauthorised access to computer material (Section 1)**
   Summary conviction (Scotland): Up to 12 months' imprisonment and/or an unlimited fine.
   On indictment: Up to 2 years' imprisonment and/or an unlimited fine.
2. **Unauthorised access with intent to commit or facilitate commission of further offences (Section 2)**
   Summary conviction (Scotland): Up to 12 months' imprisonment and/or an unlimited fine.
   On indictment: Up to 5 years' imprisonment and/or an unlimited fine.
3. **Unauthorised acts with intent to impair, or with recklessness as to impairing, the operation of a computer (Section 3)**
   Summary conviction (Scotland): Up to 12 months' imprisonment and/or an unlimited fine.
   On indictment: Up to 10 years' imprisonment and/or an unlimited fine.

Other Legal References
Data Protection Act 2018 and UK GDPR

- The policy correctly highlights the need to protect personal data. You might consider explicitly naming it the **"UK GDPR"** (post-Brexit term) rather than EU GDPR.

- Data Protection Act 2018 and GDPR:
  The Data Protection Act and GDPR controls how personal and sensitive data is used by organisations, businesses or the government. Everyone responsible for using data has to follow strict rules called 'data protection principles'.

- Communications Act 2003 (section 127)
  The Communications Act 2003 is a British Act of Parliament. The act, which came into force on 25 July 2003, superseded the Telecommunications Act 1984. It consolidated the telecommunication and broadcasting regulators in the UK, introducing the Office of Communications (Ofcom) as the new industry regulator.

31. Users must ensure that they do not breach any copyright or other intellectual property rights when creating and/or sending communications, as this is illegal.

32. Before sending an email or text users must check that it is the most appropriate method of communication compared to e.g. a telephone call, meeting, memo or letter, particularly where prompt communication and reply are needed.

33. All emails should be proof read before transmission, including ensuring that any attachments referred to in the text are correctly attached and that the intended recipient's email address is correct.

34. Each email to an external address should contain the Association's disclaimer notice, which should be added automatically by the system. Any user becoming aware that the disclaimer has not been added should advise their line manager immediately.

35. If an important document is transmitted by email, the sender should request a 'read receipt' to confirm the document has been received and may also wish to follow up with a phone call to ensure safe delivery in full.

36. All users must ensure that they apply the same 'quality control' standards to advice given by email or text as they do to advice given in any other form of communication. Users should be aware that the risk of exposing the Association to claims of negligence is as great using emails/texts as through any other means.

37. All users must carry out regular 'housekeeping' on their email folders to keep them at a reasonable size. Unwanted mail must be deleted immediately. If information is to be kept it should be stored in an appropriate file in the system, ensuring compliance with GDPR.

38. Unsolicited mail or mail from an unknown source must be treated with caution. If in doubt a user receiving such mail must contact our IT Support provider or a member of the Senior Management Team before opening the email.

39. Before opening any attachment from an external source, the user must satisfy themselves that they know what it should contain and if in any doubt about the safety of opening the attachment must contact our IT Support provider or a member of the Senior Management Team.

40. Users must not send emails from their work computer, or texts from their work phone or any other communication device provided by the Association, containing damaging, untrue, rude, abusive, defamatory, libellous or

harassing material about any individual, firm or other organisation. **Under no circumstances** will any such views be expressed via the Association's email or text systems. Please refer to the Association's 'Communications Tools Policy' for further information.

41. Users must not use or associate their Association email address for accessing social networks or other non-business websites.

42. Users must not:

- send files via the internet that are available either as a commercial product or are freely available, such as computer games, screen savers, bit maps etc.;

- send or forward 'junk mail', especially chain letters;

- send or receive personal emails using their Association email address, or give out their business email address to non-business contacts for sending personal emails to the user;

- email business documents to their own or a colleague's personal web-based email account - unless there is a business reason for doing so, such as keeping a colleague on maternity leave up to date with relevant matters.

ACCESSING WEBSITES

43. During working hours, users must only access internet sites primarily for business use, to enable them to carry out their duties.

44. Users must not deliberately access or attempt to access inappropriate internet sites or obtain material that is illegal or inappropriate to their work and which may cause embarrassment to the Association's corporate image. This includes downloading apps to devices owned by the Association. Please refer to the Association's 'Communications Tools Policy' for more information.

45. Should a user access such a website accidently they must immediately inform a member of the Senior Management Team.

46. Users may use their work computer or communications device to access the internet to purchase goods or services for personal use, **so long as:**

- they do so out-with working hours or during their lunch break; **and**

- they use their **personal** email account and **not** their Association business

address, i.e. personal goods must not be purchased using an Association email address.

USE OF 'BLOGS' & SOCIAL NETWORKING SITES

47. Access to and the use of 'blogs' and social networking sites will be governed by the following principles:

- **During working hours** (with the exception of authorised work-related 'social media')
  Users **will not view or contribute to** blogs, content sharing and social networking sites such as 'Facebook', 'Instagram', 'Twitter' and 'YouTube' using the Association's computer and communications systems **or** their personal communications devices.

- **Out-with working hours & during lunch break**
  Users may view and contribute to blogs and social networking sites from the Association's equipment, **but only if** they access such sites from their **personal email accounts** and not from any Association business address, and if they comply with this policy regarding not accessing or posting inappropriate or illegal material.

48. When contributing to websites, users must always ensure that their conduct is appropriate and consistent with their contract or appointment, and that they do not bring any disrepute to the Association's name. If there is any likelihood that the content could identify the user with the Association, the user must ensure that a disclaimer is added stating that the views expressed are those of the individual and do not represent the Association's views.

49. Users must not make any defamatory, actionable or untrue statements about colleagues or anyone else associated with the Association, or about their work or the organisation, on any blogs, content sharing or social networking sites, either within or out-with working hours.

MISUSE & ENFORCEMENT

50. Any user found to be misusing the Association's communications equipment and systems will be dealt with in accordance with current disciplinary, governance or contractual procedures.

51. Any user who knows or suspects that a colleague (of whatever seniority) is misusing the computer or communications systems should approach the Director (or the Chairperson of the Management Committee in the case of the Director) for a confidential discussion. If necessary, staff or Committee members should use our Whistleblowing policy.

52. Where there is a clear instance of misuse or abuse of equipment of systems, or any other non-compliance with this policy (or the Association's Communications Tools Policy), this may result in the withdrawal of facilities in addition to any disciplinary action taken.

53. Where a criminal offence may have been committed, the Director in consultation with the Chairperson will decide whether to involve the Police (in some clearly illegal instances there will be a requirement to report the matter promptly to the Police).

IMPLEMENTATION & REVIEW

54. The Director has overall responsibility for the security of computer systems and the implementation of this policy.

55. Line Managers are responsible for the implementation of this policy within their teams.

56. All users are responsible for ensuring that they comply with this policy when using the Association's computer and related communications systems.

57. The Director will regularly monitor the implementation of the policy and will report any breach of the policy to the Management Committee.

58. In implementing this policy, we will ensure we comply with relevant equalities legislation.

59. The Director will ensure that this policy is reviewed at least every three years by the Management Committee, or earlier if there is a relevant legislative or best practice change.