The Walled Garden Studio, Alscot Park, Stratford upon Avon, CV37 8BL

E: toby@hawkscroft.com - T: 01608 637148

HAWKSCROFT LIMITED - CYBER & ICT SECURITY POLICY

Title	Cyber & ICT Security Policy
Issue date	01.01.2024
Revision date	01.01.2025
Version	V7
IT Security Manager	Barry T Cubitt (Security4Systems)
Data Protection Manager	Toby I B Jones

Contents

1. Introduction

1.1 All information held by Hawkscroft Ltd, in all formats, represents an extremely valuable asset and, therefore, must be used and stored in a secure manner.

1.2 This Policy is in two parts, the first outlines security procedures covering all aspects of processing information. The second part covers security of IT systems.

1.3 The Policy must be read in conjunction with Hawkscroft Ltd Data Protection Policy.

1.4 The Policy applies to all operatives, subcontractors and employees of Hawkscroft Ltd both permanent and temporary and also applies to contractors employed by Hawkscroft Ltd engaged to work with or who have access to our data and/or information, i.e. IT Security/Computer Repair & Maintenance Consultants.

1.5 The Policy applies to all locations from which Hawkscroft Ltd systems are accessed (including home use).

1.6 Suitable third party processing agreements must be in place before any third party is allowed access to personal information for which Hawkscroft Ltd is responsible.

2. Policy Compliance

2.1 The Information Security Manager will ensure that all operatives are aware of and understand the content of this policy, as necessary and according to their roll.

2.2 If any user is found to have breached this policy, they could be subject to disciplinary procedure and possible dismissal. Serious breaches of this policy will be regarded as gross misconduct.

3. Legal Aspects

3.1 Some aspects of information security are governed by legislation; the most notable UK Acts and European legislation are listed below:

- The Data Protection Act (2018)
- General Data Protection Regulation (GDPR)
- Copyright, Designs and Patents Act (1988)
- Computer Misuse Act (1990)

4. Responsibilities

4.1 Managers must:

- Be aware of information or portable ICT equipment which is removed from Hawkscroft Ltd systems and manage securely
- Ensure all operatives, whether permanent or temporary, are instructed in their security responsibilities
- Ensure operatives using computer systems/media are trained in their use

- Determine which individuals are given authority to access specific information and security systems. The level of access to specific systems should be on a job function need, irrespective of status
- Ensure staff are unable to gain unauthorised access to confidentially categorised IT and security systems or manual data
- Implement procedures to minimise Hawkscroft Ltd exposure to fraud, theft or disruption of its systems
- Ensure current documentation is maintained for all critical job functions to ensure continuity in the event of relevant operative(s) being unavailable
- Ensure that the relevant system administrators are advised immediately about changes of operatives affecting computer access i.e. job function changes leaving business unit or organisation, so that passwords may be withdrawn or changed as appropriate
- Ensure that all contractors undertaking work for Hawkscroft Ltd have signed confidentiality (non-disclosure) undertakings - where relevant
- Ensure Hawkscroft Ltd Clear Desk Policy is enforced, particularly in relation to confidential or personal information. The Clear Desk Policy can be found in Section 11 below
- Ensure information held is accurate, up to date, and retained, in line with compliant retention and disposal
- Ensure relevant staff and operatives are aware of, and comply with, any restrictions specific to their role or service area i.e. Memoranda of Understanding with Government Departments, Data Sharing and Confidentiality & Non-disclosure Agreements to which Hawkscroft Ltd is a signatory

4.2 The IT Security Manager and staff/operatives are responsible for:

- Ensuring that no breaches of information security result from their actions, reporting any breach or suspected breach of security without delay.
- Ensuring information they have access to remains secure. The level of security will depend on the sensitivity of the information and any risks which may arise from its loss
- Ensuring they are aware of and comply with any restrictions specific to their role or service area i.e. Memoranda of Understanding with Government Departments, Data Sharing and Confidentiality & Non-disclosure Agreements to which Hawkscroft Ltd is a signatory

4.3 All staff/operatives should be aware of confidentiality agreements with Hawkscroft Ltd in their conditions of contract – where applicable.

4.4 Advice and guidance regarding IT Security, use of information and Data Protection can be provided by the IT Manager and Data protection Manager.

...continued

PART 1 - KEEPING INFORMATION SECURE

5. Data Protection by Design and Default

5.1 The General Data Protection Regulation (GDPR) requires that organisations put in place appropriate technical and organisational principles and safeguard individual rights. This is known as 'data protection by design and by default'. This means that we have to integrate data protection into our processing activities and business practices, from the design stage right through the lifecycle.

5.2 Hawkscroft Ltd will therefore ensure that privacy and data protection is a key consideration in everything we do. As part of this we will:

- consider data protection issues as part of the design and implementation of systems, services, products and business practices
- make data protection an essential component of the core functionality of our processing systems and services
- anticipate risks and privacy-invasive events before they occur and take steps to prevent harm to individuals
- only process the personal data that we need for our purpose(s) and that we only use the data for those purposes

5.3 Core privacy considerations should be incorporated into existing project management and risk management methodologies and policies to ensure:

- Potential problems are identified at an early stage
- Increased awareness of privacy and data protection
- Legal obligations are met and data breaches are minimised
- Actions are less likely to be privacy intrusive and have a negative impact on individuals

6. Data Breaches and Information Security Incidents

6.1 Hawkscroft Ltd has a duty to ensure that all personal information is processed in compliance with the principles set out in the General Data Protection Regulation (GDPR). It is ultimately the responsibility of The IT Security Manager to ensure that the company and all its operatives comply with that duty and that suitable procedures are in place for staff/operatives to follow when dealing with personal information.

6.2 Reporting of Security Incidents

It is the responsibility of each employee or contractor to report perceived security incidents on a continuous basis to the appropriate supervisor or security person. A User is any person authorized to access an information resource. Users are responsible for the day-to-day, hands-on security of that resource. Users are to formally report all security incidents or violations of the security policy immediately to the IT Security Manager and Data Protection Manager.

Reports of security incidents shall be escalated as quickly as possible. The IT Security Manager and Data Protection Manager must inform Company Directors rapidly as possible. Each incident will be analysed to determine if changes in the existing

security structure are necessary. All reported incidents are logged and the remedial action indicated. It is the responsibility of the IT Security Manager to provide training on any procedural changes that may be required as a result of the investigation of an incident.

Security breaches shall be promptly investigated and any affected third parties notified. If criminal action is suspected, the IT Security Manager shall contact the appropriate law enforcement and investigative authorities immediately, which may include but is not limited to the police or appropriate criminal investigative authorities.

7. Access control

7.1 Staff/operatives and IT contractors etc should only access systems for which they are authorised. Under the Computer Misuse Act (1990) it is a criminal offence to attempt to gain access to computer information and systems including security systems and security cameras for which they have no authorisation. All contracts of employment and conditions of contract for contractors should have a non-disclosure clause, which means that in the event of accidental unauthorised access to information (whether electronic or manual), the member of staff or contractor is prevented from disclosing information which they had no right to obtain.

7.2 Formal procedures will be used to control access to systems. Access privileges will be modified/removed as appropriate when an operative changes roll or leaves.

7.3 Staff/operatives and contractors must comply with Hawkscroft Ltd ICT Policy in relation to passwords.

7.4 Particular attention should be paid to the return of items which may allow future access. These include personal identification devices, access cards, keys, passes, manuals & documents.

7.5 Once an employee has left, it can be impossible to enforce security disciplines, even though legal process. Many cases of unauthorised access into systems and premises can be traced back to information given out by former employees.

7.6 System administrators will delete or disable all identification codes and passwords relating to members of staff or operatives who leave the employment of Hawkscroft Ltd on their last working day. The employee's manager should ensure that all PC files are transferred to another user before the member of staff leaves.

7.7 Managers must ensure that staff leaving Hawkscroft Ltd employment do not inappropriately wipe or delete information from hard disks. If the circumstances of leaving make this likely then access rights should be restricted to avoid damage to Hawkscroft Ltd information and equipment.

7.8 There is a requirement for system administrators to have a procedure in place for the secure control of contractors called upon to maintain and support computing equipment security equipment and software. The contractor may be on site or working remotely via a communications link. Hawkscroft Ltd IT Security Consultant will advise on the most suitable control.

7.9 Physical security to Hawkscroft Ltd office area(s) is provided through an access control system i.e. no one other than Hawkscroft Ltd staff is permitted on office premises.

8. Security of Equipment

8.1 Portable computers must have appropriate access protection, for example passwords and encryption, and must not be left unattended in public places.

8.2 Computer equipment is vulnerable to theft, loss or unauthorised access. Always secure laptops and handheld equipment when leaving an office unattended and lock equipment away when you are leaving the office.

8.3 Due to the high incidence of car thefts laptops or other portable equipment must **never** be left unattended in cars or taken into vulnerable areas.

8.4 Users of portable computing equipment are responsible for the security of the hardware and the information it holds at all times on or off Hawkscroft Ltd sites or premises. The equipment should only be used by the individual to which it is issued, be maintained and batteries recharged regularly.

8.5 Staff working from home must ensure appropriate security is in place to protect Hawkscroft Ltd equipment or information. This will include physical security measures to prevent unauthorised entry to the home and ensuring Hawkscroft Ltd equipment and information is kept out of sight.

8.6 Hawkscroft Ltd issued equipment must not be used by non-Hawkscroft Ltd staff/operatives.

8.7 All of the policy statements regarding the use of software and games apply equally to users of portable equipment belonging to Hawkscroft Ltd.

8.8 Users of this equipment must pay particular attention to the protection of personal data, commercial and any other sensitive data. The use of a password to start work with the computer when it is switched on, known as a 'power on' password, is mandatory and all sensitive files must be password protected if encrypting the data is not technically possible. The new user will refer to the instruction book to learn how to apply these passwords or may make arrangements for basic training in the use of a portable computer.

8.9 Users of portable equipment away from Hawkscroft Ltd premises should check their car and home insurance policies for their level of cover in the event of equipment being stolen or damaged and take appropriate precautions to minimise risk of theft or damage.

8.10 Staff/operatives who use portable computers belonging to the Hawkscroft Ltd must use them solely for business purposes.

9. Payment Card Industry (PCI) Compliance

9.1 Hawkscroft Ltd does not receive payment by debit card, credit card or any other type of payment card.

10. Security and storage of information

10.1 All information, whether electronic or manual, must be stored in a secure manner appropriate to its sensitivity. The IT Security Manager will determine the sensitivity of the information held and the relevant storage appropriate to that information. Suitable storage and security will include:

- Paper files stored in lockable cupboards or drawers
- Laptops stored in lockable cupboards or drawers
- Electronic files password protected or encrypted
- Restricted access to ICT and security systems & apps including security cameras
- Computer screens to be 'locked' whenever staff leave their desk
- Removable media to be kept in lockable cupboards or drawers and information deleted when no longer required
- Paper files removed from the office (for site visits or when working from home) to be kept secure at all times and not left in plain sight in unattended vehicles or premises
- Laptops must **never** be left in unattended vehicles
- It is advisable that paper files containing personal or sensitive data are kept separate from laptops, particularly when working from home
- At no time should sensitive, confidential or personal information be stored on a portable unit's hard drive. Access to this type of information must always be through Hawkscroft Ltd main office system
- To preserve the integrity of data, frequent transfers must be maintained between portable units and the main Hawkscroft Ltd computer system
- Staff/operatives should be aware of the position of their computer screen(s) and take all necessary steps to prevent unauthorised persons, visitors or others from being able to view the content of computers or hard copy information

11. Clear Desk Policy

11.1 Staff/operatives are required to clear working documents, open files, and other paperwork from their desks, working surfaces and shelves at the end of each working day and to place them securely into desk drawers and cupboards as appropriate.

11.2 Although security measures are in place to ensure only authorised access to office areas, staff/operatives should ensure that documents, particularly of a confidential nature are not left lying around.

11.3 Staff/operatives must ensure that documents are carefully stored. When properly implemented, this clear desk policy also improves efficiency as documents can be retrieved more easily.

12. Posting or Emailing Information

12.1 If information is particularly sensitive or confidential the most secure method of transmission must be selected. The following procedures should be adopted as appropriate, depending on the sensitivity of the information.

12.2 Please consider the risk of harm, distress or breach of confidentiality and non-disclosure that could be caused if the information was lost or sent to another person, and then look at the most appropriate way of sending the information to the recipient.

12.3 It is important that only the minimum amount of personal or sensitive information is sent, by whichever method is chosen.

12.4 Sending information by email:

- Carefully check the recipient's email address before pressing send – this is particularly important where the 'to' field autocompletes
- If personal or sensitive information is regularly sent via email, consider disabling the auto complete function and regularly empty the auto complete list. Both of these options can be found in Outlook under 'file', 'options' and 'mail'
- Take care when replying 'to all' – do you know who all recipients are and do they all need to receive the information you are sending
- If emailing sensitive information, password protect any attachments. Use a different method to communicate the password i.e. telephone call, messenger or text
- Consider the use of secure email where this is available or use drop off and encrypt the document

12.5 Sending information by post:

- Check that the address is correct
- Ensure only the relevant information is in the envelope and that someone else's letter hasn't been included in error
- If the information is particularly sensitive or confidential, discuss the most secure method of delivery with the Data protection Manager, this could be by Special Delivery or even courier

12.6 Printing and Photocopying:

- All printing must be via Hawkscroft Ltd main office printers
- Consideration must be given to using anything other than the Hawkscroft Ltd main office for large print runs, especially where personal information is concerned
- When printing or photocopying multiple documents, ensure you separate them when you return to your desk
- If the copier jams please remove all documents – if the copier remains jammed report it to Hawkscroft Ltd IT Security & Maintenance Consultant, if relevant leave your contact details on the copier so that once it has been fixed any remaining copying can be returned to you. If possible, cancel your print run.
- Make sure your entire document has copied or printed – check that the copier has not run out of paper. This is particularly important when copying or printing large documents. Please bear in mind the printer will sometimes pause in the middle of a large print run

- Do not leave the printer unattended when you're using it – someone else may come along and pick up your printing by mistake

13. Redacting

13.1 If it is necessary to redact information ensure a suitable and permanent redaction method is used.

13.2 The use of black marker pen is **not** a suitable method of redaction.

13.3 It is not advisable to change the colour of text i.e. white text on a white background or use text boxes to cover text as these can be removed from electronic documents. However, if this is the only option, once redacted the document should be printed and then scanned as a PDF before being sent.

14. Sharing and Disclosing Information

14.1 Hawkscroft Ltd will not disclose any information to a third party unless it appertains to a request for disclosure under GDPR legislation in which case it will be scrutinised in order to conform to the Data Protection Act and any Memoranda of Understanding with Government Departments, Data Sharing and Confidentiality & Non-disclosure Agreements to which Hawkscroft Ltd is a signatory.

14.2 Notwithstanding section 14.1, if a request for disclosure of information is received from a third party Hawkscroft Ltd will:

- Obtain a written request from the client/party
- Verify their identity, particularly if they request information via the telephone or in person. It is preferable to telephone the person back, using a recognised telephone number for their organisation (for example 101 for the Police). Do not take their mobile number and use that.

14.3 In all circumstances Hawkscroft Ltd will ensure that it is legally able to share the information being requested and only share the minimum amount of information necessary. Hawkscroft Ltd will never share any information that is governed by Memoranda of Understanding with Government Departments and Confidentiality & Non-disclosure Agreements to which is a signatory.

15. Retention and Disposal of Information

15.1 Information must only be retained for as long as it is needed for business purposes, or in accordance with any statutory retention period.

15.2 When disposing of information the most appropriate method must be used. Paper files containing personal or sensitive information must be shredded using the Hawkscroft Ltd main office shredder and electronic information must be permanently destroyed using unrecoverable delete process. Any information held by Hawkscroft Ltd under Confidentiality & Non-disclosure Agreements to which is a signatory will be given special protection and disposed of according to the required protocol within

those agreements and/or in the methods outlined in this section if permitted by those agreements.

15.4 When purchasing new computer systems, security systems or software Hawkscroft Ltd will consider requirements for the retention and disposal of information and ensure these are included at specification to the required levels of security.

16. Vacating Premises or Disposing of Equipment

16.1 It is important that a process is in place to ensure all Hawkscroft Ltd information is removed from premises should they be vacated and from equipment before it is disposed of. Equipment includes cupboards and filing cabinets as well as computers or other electronic devices.

16.2 The disposal of computer or other electronic devices is referenced in Section 25 of this policy and all electronic equipment must be returned to Hawkscroft Ltd IT Consultant to be properly disposed of.

16.3 If Hawkscroft Ltd vacates any of its premises the IT Security Manager must undertake appropriate checks of all areas, including locked rooms, basements and other storage areas, to ensure all Hawkscroft Ltd information is removed. Such checks should be documented, dated and signed.

16.4 If information is bagged for disposal (whether confidential or not), this must be removed before the building is vacated.

16.5 Cupboards and filing cabinets must be checked before their disposal to ensure they contain no documents or papers. If a cupboard or cabinet is locked and no key is available, the IT Security Manager will take steps to open it in order that it can be checked.

...continued

PART 2 - ICT SECURITY

17. Cloud Storage Solutions

17.1 The use of cloud storage solutions (SkyDrive, OneDrive Personal, iCloud etc.) for the transfer of Hawkscroft Ltd ICT information is expressly forbidden.

18. Systems Development

18.1 All system developments must comply with the Hawkscroft Ltd IT Strategy. All system developments must include security issues in their consideration of new developments, seeking guidance from the IT Manager and IT Security Consultant.

19. Network Security

19.1 Hawkscroft Ltd will use their IT Security Consultant to routinely review network security. Hawkscroft Ltd system(s) utilise hard wired inter PC/router connections and uses an internal office network only.

20. Risks from Viruses

20.1 Viruses (including malware and zero day threats) are one of the greatest threats to Hawkscroft Ltd computer system(s). PC viruses become easier to avoid when staff/operatives are aware of the risks with unlicensed software or bringing data/software from outside Hawkscroft Ltd system(s). Anti-virus measures reduce the risks of damage to the system(s) and internal network.

20.2 Anti-virus and anti-malware software and programmes are maintained and updated on Hawkscroft Ltd IT system(s) but users are responsible for checking that virus updates are automatically occurring on all desktop machines. Advice and support is available from IT Security Consultant if any remedial action is necessary. Any suspected virus attacks must be reported to the IT Security Manager immediately.

21. Cyber Security

21.1 Cyber security and cybercrime are increasing risks that, if left unchecked, could disrupt the day to day operations of Hawkscroft Ltd and have the potential to compromise security.

22. Access Control to Secure Areas

22.1 Secure areas include:

- Hawkscroft Ltd main office
- Hawkscroft Ltd main office storage room

22.2 Hawkscroft Ltd main computer, storage hardware and network equipment are located in secure areas with restricted access.

22.3 Hawkscroft Ltd main computer is situated in a secure area with restricted access.

22.4 Local/internal network equipment will be located in secure areas and where appropriate within locked cabinets, security apps to be password protected.

22.5 Unrestricted access to Hawkscroft Ltd main computer will be confined to designated staff/operative(s) whose job function requires access to that particular area/equipment.

22.6 Restricted access may be given to other staff where there is a specific job function need for such access.

22.7 Authenticated representatives of third party support agencies i.e. IT Security Consultancy and maintenance contractor will only be given access through specific authorisation.

22.8 All secure areas, security systems and apps have restricted access.

22.9 Regular reviews of who can access these secure areas should be undertaken.

23. Security of Third Party Access

23.1 No external agency will be given access to any of Hawkscroft Ltd IT system(s) unless that body has been formally authorised to have access.

23.2 All external agencies will be required to sign security and confidentiality agreements with Hawkscroft Ltd.

23.3 No external agencies will process personal information on Hawkscroft Ltd behalf.

24. Data Back-up

24.1 Hawkscroft Ltd data must not be held on a PC hard drive with the approval of the IT Security Manager.

24.2 Data should be protected by clearly defined and controlled back-up procedures which will generate data for archiving and contingency recovery purposes.

24.3 All backup copies should be clearly labelled and held in a secure area. Procedures should be in place to recover to a useable point after restart of this back-up. A cyclical system, whereby several generations of backup are kept, is recommended.

24.4 Archived and recovery data should be accorded the same security as live data and stored accordingly. Archived data is information which is no longer in current use, but may be required in the future, for example, for legal reasons or audit purposes.

24.5 Recovery data should be sufficient to provide an adequate level of company service and record keeping.

24.6 Recovery data should only be accessed and used with the formal permission of the IT Security Manager

24.7 If data is corrupted it should be securely recovered or disposed of by the IT Security Consultant.

25. Equipment, Media and Data Disposal

25.1 If a computer has been used to process personal data as defined under the Data Protection Act (2018) or 'in confidence' data, then any storage media should be disposed of only after reliable precautions to destroy the data have been taken i.e. by the IT Security Consultants. Procedures for disposal should be documented on Hawkscroft Ltd disposal log.

25.2 Many software packages have routines built into them which write data to temporary files on the hard disk for their own purposes. Users are often unaware that this activity is taking place and may not realise that data which may be sensitive is being stored automatically on their hard disk.

25.3 Although software packages usually (but not always) deletes temporary files after they have served their purpose, they could be restored and retrieved from the disk by using commonly available utility software. Therefore, disposal must be arranged through IT Security Consultants who will arrange for disks to be wiped or destroyed to the appropriate standards.

26. Software

26.1 All users should ensure that they only use licensed copies of commercial software. It is a criminal offence to make/use unauthorised copies of commercial software. Each user should ensure that a copy of each licence for commercial software is held.

26.2 The loading and use of unlicensed software on Hawkscroft Ltd computing equipment is NOT allowed. All staff/operatives must comply with the Copyright, Designs and Patents Act (1988). This states that it is illegal to copy and use software without the copyright owner's consent or the appropriate licence to prove the software was legally acquired. Hawkscroft Ltd monitors the installation and use of software by means of regular software audits; any breaches of software copyright may result in personal litigation by the software author or distributor.

26.3 Hawkscroft Ltd will only permit authorised software to be installed on its computer(s). Approval will be via IT Security Manager as advised by IT Security Consultants.

26.4 Where Hawkscroft Ltd recognises the need for specific specialised PC products such products should be registered with IT Security Consultants and be fully licensed.

26.5 Software packages must comply with and not compromise Hawkscroft Ltd security standards.

26.6 Computers owned by Hawkscroft Ltd are for company use only and only to be used for company business. The copying of leisure software on to computing equipment owned by Hawkscroft Ltd is not allowed. Computer leisure software is one of the

main sources of software corruption and viruses which may lead to the destruction of complete systems and the data contained on them.

26.7 Educational software for training and instruction should be authorised, properly purchased, virus checked and loaded by the IT Security Consultants. Where a software training package includes 'games' to enable the new user to practise their keyboard skills i.e. Windows, then this will be allowed as long as it does not represent a threat to the security of the system.

26.8 Hawkscroft Ltd seeks to minimise the risks of computer viruses through education, good practice/procedures and anti-virus software positioned in the most vulnerable areas. Users should report any viruses detected/suspected on their machines immediately to the IT Security Manager.

26.9 Users must be aware of the risk of viruses from email and the internet. If in doubt about any data received please contact IT Security Manager for anti-virus advice.

27. Use of Removable Media and Apps

27.1 It is Hawkscroft Ltd policy to prohibit the use of all unauthorised removable media devices. The use of removable media devices will only be approved if a valid business case for its use is developed.

27.2 All staff/operatives and third parties must comply with the requirements regarding removable media.

27.3 Security related apps must have password protected access and are restricted to one designated user responsible for company security.

28. Timeout Procedures

28.1 Inactive computers should be set to time out after a pre-set period of inactivity. The time-out facility should clear the screen.

28.2 Users must 'lock' their computers, if leaving them unattended for any length of time.

29. System Documentation

29.1 All systems should be adequately documented by the IT Security Manager and should be kept up to date so that it matches the state of the system at all times.

29.2 System documentation, including manuals, should be physically secured (for example, under lock and key) when not in use.

29.3 General Internet access carries with it a security risk of downloading viruses or programs that can look around a network and infiltrate password security systems. This information can then be sent back to the originator of the program in order to allow them unauthorised access to our systems. Therefore no data should be transferred between Hawkscroft Ltd computer system(s) and home PCs or laptops.

END