The Steadfast Security Group

Data Protection & Data Security Policy

1 Hackworth Road,
Northwest Industrial Estate
Peterlee
County Durham
SR8 2JQ

Tel: 0191 518 0837
Email: contact@steadfastsecurity.co.uk
Web: www.steadfastsecurity.co.uk

SSG.I.0052

GENERAL INFORMATION			
Organisation:	**Steadfast Security Group**		
Version:	**01**	**Document Owner:**	**Compliance Manager**
Issue Date:	**02 October 2025**	**Next Review:**	**02 October 2028**
Email Address:	**Steven.hope@steadfastsecurity.co.uk**	**Tel Number:**	**0191 518 0837**

AMENDMENTS				
Ser No	**Section**	**Reason for Amendment**	**Amended By**	**Date**

REVIEWS				
Ser No	**Date**	**Reason for Review**	**Reviewed By**	**Next Review**

SCOPE

1. **Steadfast Security Group** (Steadfast), comprising **Steadfast Security Solutions Limited** (Solutions), **Steadfast Security Systems Limited** (Systems), **Steadfast Secure Storage Limited** (Storage), and **Complete Security (Europe) Limited** (Complete), is committed to ensuring that all personal data is processed in accordance with legally compliant standards of data protection and data security.

2. For the purposes of applicable data protection laws, Steadfast acts as the data controller in relation to personal data processed in connection with employment. This means Steadfast determines the purposes for which, and the way, personal data is processed.

3. The purpose of this policy is to support Steadfast in achieving its data protection and data security objectives by:

   a. Informing staff of the types of personal data that may be held about them, customers, suppliers, and other third parties, and explaining how that data is used.

   b. Establishing clear rules on data protection and outlining the legal requirements that must be met when collecting, receiving, handling, processing, transferring, and storing personal data.

   c. Clarifying the responsibilities and obligations of staff in relation to data protection and data security.

4. This policy is a statement of intent and does not form part of any employee's contract of employment. Steadfast reserves the right to amend this policy at any time, at its sole discretion.

5. For the purposes of this policy:

   a. **Criminal records data** refers to information about an individual's criminal convictions, offences, and related allegations or proceedings.

   b. **Data protection laws** include all applicable legislation governing the processing of personal data, including the UK General Data Protection Regulation (UK GDPR), while it remains in force.

   c. **Data subject** means the individual to whom the personal data relates.

   d. **Personal data** refers to any information relating to an identifiable individual.

   e. **Processing** encompasses any activity involving personal data, including its collection, storage, amendment, disclosure, or destruction.

   f. **Special categories of personal data** include information relating to an individual's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health, sex life or sexual orientation, and biometric data.

DATA PROTECTION PRINCIPLES

6. All staff whose roles involve handling personal data—whether relating to colleagues, customers, suppliers, or other third parties—must comply with this policy and adhere to the following core data protection principles. These principles are designed to ensure that personal data is processed lawfully, securely, and responsibly:

   a. **Lawfulness, Fairness, and Transparency**: Personal data must be processed lawfully, fairly, and in a transparent manner. A lawful basis must exist for all processing activities, as defined by data protection laws. This may include processing that is necessary for the performance of a contract, compliance with a legal obligation, or the legitimate interests of the data controller or recipient. Data subjects must be informed of who controls their data (Steadfast), the purposes for which it is being processed, and any third parties to whom it may be disclosed.

b. **Purpose Limitation**: Personal data must be collected only for specified, explicit, and legitimate purposes. It must not be used for any purpose other than that originally stated, unless the data subject is informed and consents to the change.

c. **Data Minimisation**: Personal data must be adequate, relevant, and limited to what is necessary in relation to the purposes for which it is processed. Steadfast will only collect the minimum amount of data required to fulfil the stated purpose.

d. **Accuracy**: Steadfast will take all reasonable steps to ensure that personal data is accurate and kept up to date. Any inaccurate data will be rectified or deleted without undue delay. Regular checks will be carried out to maintain data accuracy.

e. **Storage Limitation**: Personal data will be retained only for as long as necessary to fulfil the purpose for which it was collected. Once no longer required, data will be securely deleted. For guidance on retention periods, staff should contact the Compliance Manager.

f. **Security**: Appropriate technical and organisational measures will be implemented to ensure the security of personal data. This includes protection against unauthorised or unlawful processing, accidental loss, destruction, or damage.

STEADFAST COMPLIANCE WITH GDPR

7. Steadfast Security Group is fully committed to complying with the requirements of the General Data Protection Regulation (GDPR). This commitment involves taking all necessary steps to ensure that personal data is handled lawfully, securely, and transparently across all areas of the business.

8. To meet these obligations, Steadfast has implemented robust processes and procedures designed to protect the personal data of staff, customers, clients, and visitors. These measures include secure methods of data collection and storage, clear communication about how personal data is used, and the provision of rights for individuals to access, amend, or request the deletion of their data.

9. Steadfast places a high priority on the protection of sensitive information and materials. To support this, the organisation follows the Privacy Compliance Framework as outlined in BS 10012:2017+A1:2018 – *Data Protection – Specification for a Personal Information Management System (PIMS)*, and ISO/IEC 27701:2022 – *Information Security, Cybersecurity and Privacy Protection – Requirements for Information Security Management Systems*. These standards provide a structured approach to managing personal data and ensuring ongoing compliance with data protection legislation.

WHO IS RESPONSIBLE FOR DATA PROTECTION AND DATA SECURITY?

10. Ensuring appropriate standards of data protection and data security is a shared responsibility between Steadfast and all members of staff. This policy applies to all individuals working within or on behalf of Steadfast, regardless of role, seniority, or employment status. This includes employees, directors, officers, consultants, contractors, agency and casual staff, trainees, homeworkers, fixed-term staff, and volunteers (collectively referred to as "Staff").

11. Any questions regarding this policy, or requests for further guidance, should be directed to the Compliance Manager.

12. All staff have a personal duty to comply with this policy, to handle personal data in accordance with the principles outlined, and to take appropriate measures to safeguard data security. Managers have an additional responsibility to lead by example, monitor compliance, and enforce the standards set out in this policy. Any suspected or actual breach of this policy must be reported to the Compliance Manager as soon as reasonably practicable.

13. Breaches of this policy are treated seriously and may result in disciplinary action, up to and including dismissal. Significant or deliberate breaches, such as unauthorised access to personal data, may constitute gross misconduct and could lead to dismissal without notice.

14. The overall responsibility for the protection of sensitive materials and personal data lies with the Board of Directors. However, operational responsibility has been delegated to the Compliance Manager.

15. The **Board of Directors** at Steadfast holds overall responsibility for the protection of sensitive materials and data. Their duties include developing and implementing an effective information security strategy, identifying and assessing data security risks, and putting in place appropriate measures to mitigate those risks. They are also responsible for ensuring compliance with relevant regulations and industry standards, leading and supporting the data protection team, and promoting a culture of data security awareness throughout the organisation.

16. The **Compliance Manager** at Steadfast is responsible for overseeing the effective management of sensitive materials and personal data. This includes creating and enforcing relevant policies, ensuring data collection methods support accuracy and legitimacy, and designing secure procedures for data handling and analysis. The role also involves establishing protocols for data sharing with senior management, supporting staff in maintaining data protection standards, and acting as the primary point of contact for supervisory authorities and internal teams. Additional responsibilities include evaluating data processing activities, advising on Data Protection Impact Assessments (DPIAs), monitoring compliance, participating in strategic meetings to embed privacy by design, and maintaining records of processing operations. The Compliance Manager must also respond to data subject requests within legal timeframes, liaise with third-party data processors, conduct audits, and recommend procedural improvements. They provide guidance on managing privacy breaches, organise GDPR training for staff, stay informed of legal developments, and issue recommendations to ensure ongoing compliance.

17. **All staff** at Steadfast are responsible for supporting the protection of sensitive information and materials. This includes notifying the organisation of any changes to their personal data, such as updated contact or banking details, and ensuring the personal data of colleagues and customers is handled with care. Staff must only access sensitive data when authorised and for legitimate business purposes and must ensure that such data is only shared with individuals who have appropriate authorisation. Personal data or devices containing such data must not be removed from Steadfast premises without implementing suitable security measures, such as encryption or password protection. Additionally, staff should avoid storing sensitive data on local drives or personal devices used for work, to maintain the integrity and security of company information.

WHAT PERSONAL DATA AND ACTIVITIES ARE COVERED BY THIS POLICY?

18. This policy applies to all personal data processed by Steadfast Security Group. Personal data refers to any information relating to a living individual who can be identified either directly from that information or indirectly when combined with other data held by Steadfast.

19. The scope of this policy includes personal data that is stored electronically or in structured paper-based filing systems. It covers both information and statements of opinion, provided they relate to an identifiable individual.

20. This policy applies to personal data concerning current, former, or prospective staff members, as well as any other individuals whose data is handled or controlled by Steadfast. It encompasses all activities involving personal data, including its collection, receipt, storage, organisation, amendment, retrieval, use, disclosure, transfer, transportation, and destruction.

21. All personal data covered by this policy is subject to the legal protections and obligations set out in applicable data protection laws. Steadfast is committed to ensuring that these standards are upheld across all data processing activities.

WHAT PERSONAL DATA DO WE PROCESS ABOUT STAFF?

22. Steadfast Security Group collects and processes personal data about staff from a variety of sources. This includes information:

a. Provided directly by the individual before or during their employment or engagement with Steadfast.

b. Supplied by third parties, such as references from previous employers, or information received from suppliers or business partners.

c. Available in the public domain.

23. The types of personal data we may collect, store, and use include, but are not limited to, the following:

a. **Contact Information**: Home address, personal contact details, and emergency contact information for next of kin.

b. **Recruitment Records**: Application forms, CVs, references, and details of qualifications and professional experience.

c. **Employment and Financial Data**: Pay records, National Insurance number, tax details, and information relating to employment benefits such as pensions and health insurance, including any claims made.

d. **Communication and IT Usage**: Records of telephone, email, internet, fax, and instant messaging usage where relevant to business operations.

e. **Medical Information**: Where necessary and appropriate, records relating to an individual's medical history.

f. **Performance and Conduct**: Documentation relating to performance reviews, disciplinary actions, grievances, complaints, or any concerns in which the staff member is involved.

24. All personal data processed by Steadfast is handled in accordance with applicable data protection laws and internal policies to ensure confidentiality, integrity, and lawful use.

SENSITIVE MATERIALS, INFORMATION AND PERSONAL DATA

25. From time to time, Steadfast may need to process sensitive personal information, also referred to as ***special categories of personal data***. This type of data is subject to enhanced legal protections under data protection laws and will only be processed where a lawful basis exists.

26. Sensitive personal data will only be processed if it is necessary for the performance of an employment contract or if one of the specific legal conditions for processing applies. These conditions include: the data subject providing explicit consent; the processing being required to exercise employment law rights or obligations; the protection of the data subject's vital interests where they are unable to give consent; the data being manifestly made public by the data subject; the processing being necessary for the establishment, exercise, or defence of legal claims; or the processing being required for reasons of substantial public interest.

27. Before any sensitive personal data is processed, staff must notify the Compliance Manager. The Compliance Manager will assess whether the proposed processing meets the legal criteria and ensures the individual concerned is properly informed of the nature, purpose, and legal basis for the processing.

28. Further details regarding the types of sensitive personal data Steadfast may process, the purposes for which it is used, and the lawful basis for doing so are outlined in the company's Privacy Notice.

CRIMINAL RECORDS INFORMATION

29. Steadfast processes criminal records information in accordance with its Criminal Records Information Policy. This ensures that any data relating to criminal convictions, offences, or related proceedings is handled lawfully, securely, and in line with applicable data protection legislation and internal standards.

HOW WE USE YOUR PERSONAL DATA

30. Steadfast Security Group is committed to processing personal data lawfully and transparently. The reasons for processing your personal data, the ways in which it is used, and the legal basis for doing so are outlined in our Privacy Notice. We will not use staff personal data for any purpose other than those specified.

31. Generally, personal data is used to support the effective operation of our business, manage your employment or engagement, and address any concerns or issues that may arise. This includes, but is not limited to:

a. **Contact Information**: Maintaining staff address lists to enable communication outside of working hours when necessary.

b. **Health Records**: Recording sickness absence, storing medical documentation such as doctor's notes, notifying colleagues of absences, managing absence levels, addressing patterns of concern, and supporting performance appraisals. Aggregated and anonymised sickness data may also be published internally.

c. **IT Monitoring**: Monitoring the use of company communication systems, including email, internet, telephone, fax, and other IT resources, to ensure appropriate use.

d. **Employee Relations**: Managing disciplinary, grievance, legal, regulatory, or compliance matters involving staff.

e. **Performance Management**: Conducting performance reviews and assessments.

f. **Equal Opportunities Monitoring**: Collecting data for equality monitoring purposes and publishing anonymised, aggregated workforce statistics.

32. All personal data is processed in accordance with applicable data protection laws and internal policies to ensure confidentiality, integrity, and lawful use.

ACCURACY AND RELEVANCE

33. Steadfast is committed to ensuring that all personal data processed is accurate, up to date, adequate, relevant, and not excessive in relation to the purpose for which it was collected. Personal data obtained for one specific purpose will not be used for any other purpose unless the individual has given consent or would reasonably expect such use. If you believe that any personal information held about you is inaccurate or outdated, you should notify the Compliance Manager. Where the Compliance Manager agrees, the information will be corrected promptly. If the correction is not agreed upon, your comments will be recorded alongside the existing data.

STORAGE AND RETENTION

34. All personal data, including sensitive personal information, is stored securely in accordance with Steadfast's Information Security Policy. The duration for which personal data is retained is determined by the nature of the data and the purpose for which it was collected. Specific retention periods are outlined in our Privacy Notices, which ensure compliance with legal obligations and support responsible data management practices.

INDIVIDUAL RIGHTS

35. Under data protection laws, you have several rights in relation to your personal data. These rights are designed to give you greater control over how your information is used and ensure transparency in our data processing activities.

SUBJECT ACCESS REQUESTS

36. You have the right to request access to the personal data we hold about you. Upon making a subject access request, we will confirm whether your personal data is being processed and, if so, provide details including: the purpose of the processing, the categories of data involved, the source of the data (if not collected directly from you), any

recipients or categories of recipients to whom the data has been disclosed, the retention period or criteria used to determine it, your rights to rectification, erasure, restriction or objection, your right to lodge a complaint with the Information Commissioner, and whether any automated decision-making is involved, including the logic behind such decisions.

37. We will also provide you with a copy of the personal data undergoing processing, typically in electronic format if the request was made electronically, unless you request otherwise. To make a subject access request, please contact us at personnel@steadfastsecurity.co.uk or steven.hope@steadfastsecurity.co.uk We may require proof of identity before processing your request and will inform you of the documents needed. We aim to respond within 28 days of receiving your request. In cases involving large volumes of data, we may take up to three months but will notify you within the initial 28-day period if this applies. If a request is manifestly unfounded or excessive, we reserve the right not to comply.

OTHER RIGHTS

38. In addition to access, you have the right to request that we:

a. Rectify inaccurate or incomplete personal data.

b. Erase personal data that is no longer necessary for the purposes for which it was collected.

c. Restrict or stop processing where your interests override our legitimate grounds for processing.

d. Temporarily suspend processing if the data is inaccurate or if there is a dispute regarding the legal basis for processing.

39. To exercise any of these rights, please contact personnel@steadfastsecurity.co.uk or steven.hope@steadfastsecurity.co.uk

DATA SECURITY

40. Steadfast Security Group is committed to protecting personal data through appropriate technical and organisational measures. These safeguards are designed to prevent unauthorised or unlawful processing, as well as accidental loss, destruction, or damage of personal information.

41. Maintaining data security involves ensuring that only authorised individuals have access to personal data, that data is pseudonymised or encrypted where possible, and that it remains accurate and suitable for its intended purpose. Authorised personnel must be able to access data when required for legitimate business purposes. By law, Steadfast must secure personal data throughout its lifecycle, from collection to destruction, using appropriate procedures and technologies.

42. Personal data must not be transferred to any third party for processing unless that party has agreed to comply with Steadfast's data security procedures or has demonstrated that adequate safeguards are in place.

43. Security procedures include:

a. Locking desks and cupboards that contain confidential information.

b. Securing computers with strong, regularly updated passwords and ensuring they are locked or shut down when unattended. Staff must use discretion when viewing personal data on screens to prevent unauthorised viewing.

c. Encrypting or password-protecting data stored on CDs, USB drives, or other portable media, and storing them securely when not in use.

d. Obtaining approval from the Compliance Manager before using any cloud-based storage solutions.

e. Avoiding the storage of sensitive data on mobile devices such as laptops, tablets, or smartphones.

f. Ensuring all servers containing personal data are protected by security software and located in secure areas away from general office space.

g. Backing up data regularly in accordance with Steadfast's backup procedures.

44. **Telephone Precautions**: Staff handling telephone enquiries must take care to avoid inappropriate disclosures. The identity of the caller must be verified before any personal data is shared. If verification is not possible, the caller should be asked to submit their query in writing. Staff must not be pressured into disclosing information and should contact the Compliance Manager if unsure.

45. **Methods of Disposal**: When personal data is no longer required, it must be securely destroyed. Paper documents should be shredded, and physical storage devices such as CDs or USB drives must be rendered permanently unreadable.

DATA IMPACT ASSESSMENTS

46. Certain data processing activities carried out by Steadfast may present risks to individual privacy. Where a proposed activity is likely to result in a high risk to the rights and freedoms of staff or other data subjects, Steadfast will conduct a Data Protection Impact Assessment (DPIA). This assessment will evaluate the necessity and proportionality of the processing, considering the intended purpose, potential risks to individuals, and the measures that can be implemented to mitigate those risks. DPIAs are an essential part of our commitment to privacy by design and help ensure compliance with data protection legislation.

DATA BREACHES

47. In the event that Steadfast identifies a breach of staff personal data that poses a risk to the rights and freedoms of individuals, the incident will be reported to the Information Commissioner's Office (ICO) within 72 hours of discovery, in accordance with legal requirements.

48. All data breaches, regardless of their impact, will be documented in line with Steadfast's Breach Response Policy. This ensures a consistent and accountable approach to managing and learning from such incidents.

49. Where a breach is likely to result in a high risk to the rights and freedoms of affected individuals, Steadfast will notify those individuals directly. This notification will include details of the breach, its potential consequences, and the mitigation measures taken to reduce any harm.

IT DATA SECURITY

50. Steadfast Security Group maintains robust IT data security measures to protect systems and personal data from unauthorised access, cyber threats, and data breaches. **Firewall protection** is provided under our service agreement with Bluecom, ensuring a secure perimeter around our network infrastructure.

51. All devices are safeguarded by business-grade **antivirus software** (ESET Antivirus 6+), also managed by Bluecom. These security services help prevent viruses, hacking attempts, spam, phishing, and other forms of malware or cyber-attacks.

52. Staff wishing to use **personal laptops or workstations** within the workplace must obtain prior approval from the Compliance Manager. Any personal equipment must run the latest operating system, or the same system used by Steadfast, and be equipped with antivirus software capable of protecting against malware.

53. All Steadfast systems are protected by **Multi-Factor Authentication (MFA)**, and it is mandatory for all users to install the Microsoft Authenticator application to access company systems securely.

54. **Password security** is essential. Computers must be locked with strong passwords that are changed regularly, and devices should be shut down or locked when left unattended. Staff must exercise discretion when viewing personal data

on screens to prevent unauthorised viewing. Passwords must never be shared or left visible at workstations under any circumstances.

TRAINING

55. Steadfast Security Group is committed to ensuring that all staff understand their responsibilities under data protection legislation. As part of this commitment, data protection training is provided during the induction process and at regular intervals thereafter.

56. All staff are required to complete the **Data Protection and GDPR Awareness** course annually. This 90-minute training session, developed by HSQE, may be delivered as a toolbox talk or completed individually online. The course is designed to raise awareness of data protection and the General Data Protection Regulation (GDPR), helping staff understand how to handle personal data securely and lawfully. Training modules include key legislation, employer and employee responsibilities, data protection principles, legal grounds for processing data, data subject rights, and individual responsibilities under GDPR.

57. Staff whose roles involve regular access to personal data, or who are responsible for implementing this policy or responding to subject access requests, will receive additional training tailored to their duties. This ensures they are equipped with the knowledge and skills required to comply with data protection obligations effectively.

FEEDBACK

58. Steadfast encourages all employees to share feedback on its policies to support continuous improvement. If you have any comments, questions, or concerns regarding this policy, please contact the Compliance Manager by emailing steven.hope@steadfastsecurity.co.uk. Your input is valued and helps ensure our policies remain clear, effective, and inclusive.

APPROVAL

59. This policy has been formally approved by the Board of Directors of Steadfast Security Group and is authorised for distribution across the organisation. All employees are expected to familiarise themselves with its contents and adhere to the principles and procedures outlined herein.

Paul Harbord
Managing Director, The Steadfast Security Group
02 October 2025