Responsible Information Management & Data Protection Policy

CITY & ESSEX	Last review: May 2026	Next review: May 2027
	City & Essex Limited and all affiliated subsidiaries.	

Mission Statement

City & Essex is committed to managing information responsibly, lawfully and securely. We recognise that personal data, client information, supplier information, employee records, commercial information and operational data must be protected through clear responsibilities, appropriate controls and good judgement.

This policy sets out our overarching approach to responsible information management, data protection, information security, data retention, subject access rights, data breach response, responsible AI use and confidentiality. It is intended to sit above the detailed procedures and employee guidance available through City & Essex systems and the HR platform.

Scope

This policy applies to City & Essex Limited and all affiliated subsidiaries. It applies to employees, workers, agency workers, managers, directors, contractors, consultants, suppliers and anyone who accesses, processes or manages information on behalf of City & Essex, where relevant to their role or contractual relationship.

• Personal data relating to employees, workers, applicants, clients, suppliers, contractors and other data subjects.

• Confidential business, client, supplier, commercial, operational, financial and HR information.

• Electronic systems, email, internal messaging, internet use, video conferencing, AI tools, mobile devices, shared drives and paper records.

• Information created, received, stored, transferred, accessed, processed, retained or destroyed by City & Essex.

This policy applies whether information is held electronically, in paper format, verbally, visually, through images or video, or through third-party platforms used for business purposes.

Relationship with Existing Procedures

This policy sets out City & Essex's top-level commitments and responsibilities for responsible information management and data protection. It is supported by the Data Protection Policy, Subject Data Request Policy, Data Retention Policy, Computer, E-mail & Internet Policy, Artificial Intelligence Policy, Social Media Policy, Video Conferencing Policy, Homeworking Policy, disciplinary procedures, HR records and any relevant IT or data security controls.

This policy does not remove detailed employee-facing procedures or statutory data subject rights. Those procedures remain live and should be followed where relevant. Where a more detailed procedure applies, that procedure provides the operational controls required to implement this policy in day-to-day work.

Frameworks & Legislation

This policy is informed by applicable UK law, regulatory expectations and good practice, including where relevant:

• UK General Data Protection Regulation (UK GDPR).

• Data Protection Act 2018.

• Privacy and Electronic Communications Regulations where relevant to communications and marketing activity.

• Information Commissioner's Office guidance on data protection, accountability, data subject rights and breach reporting.

• Employment Rights Act 1996 and related employment record-keeping obligations where relevant to employee data.

• Public Interest Disclosure Act 1998 where information relates to whistleblowing or protected disclosures.

• Computer Misuse Act 1990, where relevant to unauthorised access or misuse of systems.

• ISO 27001 information security management principles. City & Essex has previously held ISO 27001:2013 certification for relevant information security management activities; any certification evidence used externally will be checked for current validity, scope, certification body and accreditation status before submission.
• City & Essex Data Protection, Subject Data Request, Data Retention, Computer & Internet, Artificial Intelligence, Social Media, Video Conferencing and Homeworking procedures.

Policy Commitments

1. Lawful and Fair Use of Information

City & Essex will process personal data lawfully, fairly and transparently. Personal data will be collected for specified, explicit and legitimate purposes, kept accurate where required, limited to what is necessary, retained only where justified and processed securely.

Employees and representatives must only access, use or share information where they have a legitimate business reason and appropriate authority to do so.

2. Data Protection and Individual Rights

City & Essex will respect data subject rights, including the right of access, correction, erasure, restriction, objection, data portability and other rights that apply under UK data protection law.

Subject access requests and related data subject requests will be handled through the appropriate procedure and coordinated by the Data Protection Manager or other authorised person. Requests will be responded to within statutory timescales unless an extension is permitted by law.

3. Information Security and Access Control

City & Essex will take reasonable precautions to protect information against unauthorised access, loss, misuse, disclosure, alteration or destruction. City & Essex maintains information security controls aligned to ISO 27001 principles, supported by internal procedures and current certification evidence where applicable. Historical or expired certification evidence will not be presented as current certification. Security controls may include password protection, access restrictions, locked storage, secure disposal, encryption where practicable, controlled data sharing and appropriate oversight of systems and third-party platforms.

Employees must not download unauthorised software, copy company data without permission, save personal data to personal devices, share information informally or remove company information from secure systems unless authorised.

4. Data Retention and Secure Disposal

City & Essex will retain information only for as long as it is needed for a lawful business, contractual, legal, regulatory or operational purpose. Employee data retention is supported by the Data Retention Policy, and further retention arrangements may apply to client, supplier, finance, contract, training, incident, H&S and ESG records.

Information that is no longer required must be disposed of securely, whether held electronically or in paper form.

5. Data Breach Identification and Response

City & Essex will maintain arrangements for identifying, recording, investigating and responding to suspected or confirmed personal data breaches. Employees must report suspected data breaches

immediately to the Data Protection Manager or other authorised contact and must preserve relevant evidence.

Where a personal data breach is likely to result in a risk to the rights and freedoms of individuals, City & Essex will assess whether notification to the Information Commissioner's Office is required within the applicable statutory timeframe.

6. Responsible Use of Technology and AI

City & Essex permits the informed and responsible use of authorised technology and AI tools where appropriate for business purposes. Employees must use AI and digital systems responsibly, lawfully and securely, and must protect confidential, personal and commercially sensitive information.

Employees must review AI outputs before relying on them, avoid entering confidential or personal data into unauthorised systems, consider bias and fairness, and use AI as a tool to support human judgement rather than replace it.

7. Confidentiality in Communications and Meetings

Employees must protect confidential information in email, internal messaging, video conferencing, telephone calls, social media, meetings and day-to-day communications. Information discussed in internal meetings, client meetings or supplier meetings must not be shared outside authorised channels.

Meetings must not be recorded or shared without appropriate authorisation or participant consent where required. Social media must not be used to disclose confidential business, client, supplier, employee or operational information.

8. Third Parties and Supplier Information

Where City & Essex shares personal data or confidential information with group companies, contractors, agents, suppliers or service providers, those parties must be expected to protect information in line with applicable law, contractual requirements and City & Essex instructions.

Third-party systems or suppliers that process data on behalf of City & Essex should be reviewed proportionately to risk, sensitivity, purpose and operational importance.

9. Homeworking, Mobile Working and Client Sites

Where employees work from home, remotely, at client sites or while travelling, they remain responsible for protecting information and following City & Essex procedures. Devices, papers, screens, conversations, files and client information must be handled securely and with appropriate regard for confidentiality.

Targets and Measurement

City & Essex will use 2024 as its ESG baseline year unless a more specific baseline is stated.

Area	Baseline / Context	Target	Deadline
Subject access and data rights	Subject Data Request procedure in place	Maintain procedures for responding to subject access and related data protection requests within statutory deadlines	Ongoing
Data breach response	Data breach identification and escalation arrangements in place	Maintain a data breach log or equivalent record and review suspected or confirmed data breaches annually	Annual
Retention controls	Employee Data Retention Policy exists; wider records to be reviewed	Review retention coverage for employee, client, supplier, contract, finance, training and operational records	End 2026
AI and digital tools	AI, computer/internet, social media and video conferencing guidance in place; ISO 27001 certification held with accreditation status to be	Review AI and information security guidance to ensure it remains accessible and relevant to employees using digital tools	End 2026

	clearly identified		
Data protection awareness	Core data protection and IT guidance available through internal systems/HR portal	Maintain employee access to core data protection, IT, AI, social media, video conferencing and confidentiality guidance	Ongoing

City & Essex will not publish confidential breach details, personal data, legally privileged material or sensitive investigation information. Reporting used for EcoVadis, ESG, client assurance or management review will be aggregated and proportionate.

Responsibilities

Managing Director

The Managing Director has ultimate accountability for this policy and for ensuring that responsible information management and data protection remain part of City & Essex's governance approach.

Data Protection Manager

The Data Protection Manager, or the person responsible for data protection on a day-to-day basis, is the policy owner and is responsible for coordinating data protection compliance, reviewing this policy, supporting subject access requests, advising on data protection risks and escalating significant issues where required.

Head of People & Culture

The Head of People & Culture supports this policy by ensuring employee-facing HR procedures, HR records, employee communications and people-management practices align with data protection and confidentiality expectations.

IT Lead or IT Support Provider

The IT Lead or IT support provider supports this policy through technical controls, system access arrangements, password and device controls, monitoring arrangements, security guidance and support for data breach investigation where relevant.

Head of ESG

The Head of ESG supports this policy where responsible information management evidence is required for EcoVadis, client assurance, supplier governance, ESG reporting, carbon reporting or sustainability-related data management.

Managers and Authorised Managers

Managers and authorised managers are responsible for ensuring that information is handled securely within their teams, that concerns are escalated, and that employees understand the procedures relevant to their role.

Employees, Workers and Contractors

Employees, workers and contractors must follow this policy and supporting procedures, protect personal and confidential information, use systems responsibly, report suspected breaches promptly and only access or share information where authorised and necessary.

Suppliers and Third Parties

Suppliers and third parties that process information for or on behalf of City & Essex are expected to protect that information in line with applicable law, contractual duties and City & Essex requirements.

Supporting Procedures and Evidence

This policy is supported by relevant procedures, controls, employee guidance, records and statutory obligations. Supporting documents and evidence may include:

• Data Protection Policy.

• Subject Data Request Policy and Subject Data Request forms.

• Data Retention Policy and retention schedules or registers.

• Computer, E-mail & Internet Policy.

• Artificial Intelligence Policy.

• Social Media Policy.

• Video Conferencing Policy.

• Homeworking Policy.

• Privacy notices, contract clauses, supplier data protection requirements and data processing arrangements where relevant.

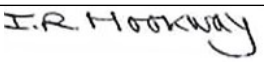
• Data breach records, subject access request records, training records, IT access records and management review evidence where available and appropriate.

These supporting documents provide the detailed controls used to implement this policy in day-to-day operations.

Reporting and Review

This policy will be reviewed annually, or sooner where required by legislation, regulatory guidance, client requirements, EcoVadis reassessment, material operational changes, data breach findings, system changes or changes to data processing activity.

Responsible information management performance will be reviewed through data protection processes, breach and concern records, subject access request handling, IT/security controls, HR procedures, supplier governance and ESG evidence review where appropriate. Significant risks or incidents will be escalated to senior leadership in line with internal procedures.

Full Name	**Mr Ian Hookway**
Position	Managing Director
Signed	
Date	May 2026