CITY & ESSEX

2026

Confidentiality & Non-Disclosure **Policy**

Document Reference: P 022
Version: V1.0



Effective Date:	October 2026	Review Date:	October 2027

1.PURPOSE AND COMMITMENT

City & Essex Ltd ("the Company") provides cleaning services to commercial clients, often within offices, retail units, managed buildings and other sensitive premises. In doing so, our people are trusted with access to client buildings, keys, access cards, alarm codes, and areas where confidential documents, equipment and personal data are present.

This policy explains how we protect the confidential information of our clients, our own business and our people. It sets out what is expected of everyone who works for or on behalf of the Company, both during and after their engagement.

Our commitment is simple: **what we see, hear or handle on a client's premises stays confidential.**

2. WHAT THIS POLICY PROTECTS

This policy is designed to protect the following aspects of client information.

2.1 Client business information

- Client identity, contract terms, pricing, rates, tender submissions and service specifications.
- Details of client operations, staffing, layouts, business plans, mergers, restructures and other commercially sensitive matters we may become aware of while on site.

2.2 Documents and materials found on premises

- Papers, files, post, whiteboards, screens, printed material, Post-it notes, waste paper and anything left on desks or in meeting rooms.
- Contents of bins, recycling and shredding bags.

2.3 Physical and site security information

- Keys, key fobs, access cards, alarm codes, lock combinations, safe locations and CCTV arrangements.
- Building layouts, security procedures, out-of-hours access arrangements and cleaning schedules.

2.4 Personal data

- Any personal data relating to a client's employees, visitors, tenants or customers that we see or handle incidentally.
- Personal data of our own staff, including right-to-work records, payroll and vetting information.

2.5 IT and electronic information

- Unlocked computers, screens, devices, USB drives, passwords written down, and any systems left accessible.
- Information sent or stored by the Company in relation to client contracts, including emails, rota systems, timesheets, photographs and audit reports.

2.6 Company confidential information

- Our own pricing, margins, methods, supplier terms, client lists, staff information and tender material.

3. DEFINITION OF CONFIDENTIAL INFORMATION

"Confidential Information" means any information, in any form (written, spoken, electronic, visual or observed), that is not publicly available and that relates to a client, the Company, or any individual, and that a person comes to know through their work with the Company. If you are unsure whether something is confidential, treat it as confidential and ask your supervisor.

4. CORE RULES FOR EVERYONE

All personnel must:

1. Not disclose Confidential Information to anyone outside the Company, including family, friends, other clients, competitors and the media, unless authorised in writing or required by law.
2. Not read, copy, photograph, remove or interfere with client documents, files, devices or personal belongings, even if left in plain view.
3. Only access areas that are within the agreed scope of work and the agreed cleaning schedule.
4. Protect keys, passes and codes at all times. They must never be shared, copied, lent, left unattended, or recorded where others can find them.
5. Not use Confidential Information for personal gain or for any purpose other than delivering the contracted service.
6. Not post about client sites, staff, premises or incidents on social media or messaging groups, and not take photographs on client premises unless this is part of an authorised task (e.g. a documented snag report) and permitted by the client.
7. Follow client-specific rules (clean desk, restricted areas, escorted access, ID requirements) which may be stricter than this policy. Where a client requires an NDA, we work to the client's own documents (see Section 8).
8. Report immediately any actual or suspected breach, lost key or pass, security incident, or suspicious activity (see Section 9).

5. HANDLING INFORMATION ON CLIENT SITES

- **Papers and documents:** Leave them exactly as found. Do not move, tidy or dispose of documents unless instructed. Only emptying of bins and designated confidential waste containers as per the agreed scope.
- **Confidential waste:** Sealed confidential waste bags and shredding containers must be left sealed and only moved as directed by the client or an authorised contractor.
- **Screens and devices:** Do not touch, switch on, move or use any computer, phone, tablet or other device other than to clean its exterior surfaces, and only where authorised.

- **Locked rooms and cabinets:** Do not attempt to open locked areas. Report any that are found unlocked or open where they would normally be secured.
- **Conversations:** Do not discuss what has been seen or heard in client premises in public places or with anyone not authorised.
- **Lone working and out-of-hours access:** Follow the client's access procedure, sign in and out where required, and lock and alarm the site on departure.
- **Visitors:** Do not allow unauthorised persons (including friends or family) onto client premises.

6. KEYS, ACCESS CONTROL AND PHYSICAL ACTIVITY

- Keys, fobs and cards are issued only to named individuals and recorded in a key register.
- Keys must be labelled in a way that does not identify the client or address to anyone who finds them.
- Alarm codes and passwords must be memorised and never written down in a way that links them to a site.
- Lost or stolen keys, cards or codes must be reported immediately (within the hour wherever possible) to the supervisor/Operations Manager so the client can be told and locks or codes changed if required.
- Keys and access items must be returned when an individual leaves the Company or is removed from a contract.
- Access to client sites is limited to the minimum number of people necessary.

7. DATA PROTECTION AND DIGITAL SECURITY

The Company complies with the UK GDPR and the Data Protection Act 2018. Where we process personal data on behalf of a client, we do so only on the client's documented instructions and in line with the data processing terms of our contract. In particular:

- Personal data is collected and kept only where necessary, held securely, and deleted when no longer needed.
- Company systems and devices used to store client information must be password protected, use up-to-date security software, and be accessible only to authorised staff.
- Client information must not be stored on personal devices or personal messaging apps unless expressly authorised.
- Emails containing client information must be sent only to the intended recipients; double-check addresses before sending.
- Paper records (e.g. site folders, timesheets, incident reports) must be kept in locked storage and securely destroyed when no longer required.
- Any personal data breach will be reported internally immediately and, where required, to the client and the Information Commissioner's Office (ICO) within 72 hours of becoming aware of it.

8. RECRUITMENT, VETTING AND CONTRACTUAL CONTROLS

- All employees and operatives sign a confidentiality undertaking / non-disclosure agreement before starting work, and the obligation continues after their employment or engagement ends.
- Appropriate pre-employment checks are carried out, including right-to-work checks, references and, where required by the client, DBS or other enhanced vetting.
- Confidentiality clauses are included in contracts of employment and in contracts with subcontractors, agency staff and suppliers, who must meet equivalent standards.
- Where a client requires a non-disclosure agreement (NDA) or has its own confidentiality requirements, the Company will work to the client's documents to ensure adherence to those specific requirements. Where the client's terms are stricter than this policy, the client's terms apply. The relevant obligations will be passed on to all staff, subcontractors and agency workers working on that contract, who must confirm they understand and will comply with them before starting work. Compliance is mandatory.

9. CONFIDENTIALITY AND SECURITY AWARENESS PROGRAMME

The Company recognises that policies only work if people understand and apply them. We therefore run an ongoing awareness programme.

9.1 Induction training.
Every new starter receives confidentiality and security training before they are given access to any client site. This covers: what counts as confidential, what to do and not do on site, key and access handling, data protection basics, social media rules, and how to report a concern. Each person signs to confirm they have understood the policy.

9.2 Site-specific briefings.
Where a client has particular requirements (restricted areas, clean desk rules, vetting, escorted access), operatives are briefed on these before starting work at that site.

9.3 Refresher training
All staff complete refresher training at least annually, and sooner after any significant incident, change in law, or change in client requirements.

9.4 Toolbox talks and reminders
Supervisors deliver short, regular talks (for example, five minutes at shift start) on topics such as secure keyholding, spotting suspicious behaviour, handling lost property, and social media. Posters and written reminders are displayed in the Company's offices and in staff rooms where practicable.

9.5 Practical scenarios.
Training uses realistic, cleaning-specific scenarios, such as finding an unlocked filing cabinet, a visitor asking to be let in after hours, a PC left logged in, or a colleague photographing a meeting room.

9.6 Accessible communication

Training and policy material is provided in plain English and, where needed, translated or delivered verbally so that all personnel can fully understand their responsibilities.

9.7 Records and monitoring

Training attendance and acknowledgements are recorded. Spot checks and site audits include confidentiality and security checks, and results are fed back into training.

9.8 Culture of speaking up

Staff are encouraged to report mistakes, near misses and concerns without fear of blame. Early reporting allows us to protect the client and put things right.

10. REPORTING AND MANAGING BREACHES

- Report immediately. Any actual or suspected breach (disclosure of information, lost keys or passes, unauthorised access, lost documents or devices, data incident) must be reported to the supervisor or Manager without delay.
- Contain. The Company will take immediate steps to limit harm, e.g. securing the site, changing locks or codes, recovering information.
- Notify. The affected client will be informed promptly in line with contract terms and legal requirements; the ICO will be notified where required.
- Investigate. The Company will establish what happened and why, keep a record, and apply corrective actions.
- Learn. Findings will be used to improve procedures and training.

No one will be penalised for reporting a concern in good faith.

11. RESPONSIBILITIES

Directors/Senior Management

Ownership of this policy, providing resources, and ensuring compliance across the business.

Operations/Contract Managers

Applying the policy on each contract, managing key registers, site briefings, audits and incident response.

Supervisors

Day-to-day enforcement, toolbox talks, spot checks, and being the first point of contact for concerns.

All Personnel

Reading, understanding and complying with this policy and reporting any concerns.

12. CONSEQUENCES OF BREACH

A breach of this policy is a serious matter. For employees it may lead to disciplinary action up to and including dismissal. For agency workers and subcontractors it may result in immediate termination of the engagement. Serious breaches may also lead to legal action, claims for damages, and, where laws such as data protection legislation are breached, regulatory action and possible personal liability.

13. DURATION OF OBLIGATIONS

Confidentiality obligations continue after employment or engagement ends, and for as long as the information remains confidential, unless the information enters the public domain other than through a breach of this policy.

14. EXCEPTIONS

Information may be disclosed where required by law, a court, or a regulator or law enforcement body. Where lawful and practical, the Company's management and the affected client will be informed before disclosure. Nothing in this policy prevents anyone from making a protected disclosure (whistleblowing) under the Public Interest Disclosure Act 1998.

15. REVIEW

This policy is reviewed at least annually, or sooner if there is a change in law, client requirements or following an incident.

Business Name: **City & Essex Ltd**
Approved and Signed By: **Ian Hookway, Managing Director**
Approval Date: **October 2026**

Email: **ian@cityanessex.com**
Phone: **01268 776 476**

APPENDIX A - EMPLOYEE CONFIDENTIALITY UNDERTAKING

I, _____ (print name), confirm that I have read and understood City & Essex Ltd's Confidentiality and Non-Disclosure Policy. I agree that:

- I will keep confidential all information I learn about clients, their premises, people and operations, and about City & Essex Ltd, during and after my work with the Company.
- I will not disclose, copy, photograph or remove any such information except as required for my work and authorised by the Company.
- I will look after all keys, passes and codes issued to me and report any loss immediately.
- I will report any breach or suspected breach straight away.
- I understand that a breach may result in disciplinary action, termination, and possible legal action.

Signature: _____ Date: _____

APPENDIX B - QUICK REFERENCES FOR SITE TEAMS

- Leave documents and devices exactly as you find them.
- Keep keys, passes and codes secure and private.
- Don't photograph, post or gossip about client sites.
- Stick to your agreed areas and times.
- Unlocked cabinet, open office or something odd? Report it.
- Lost keys or a card? Tell your supervisor straight away.
- Not sure? Treat it as confidential and ask.