Internal Policy Handbook

Version 2.0 - January 2025

Classification: INTERNAL

1. Introduction and Scope

This Internal Policy Handbook outlines the policies, procedures, and standards that govern employee conduct and organisational operations. It applies to all full-time, part-time, and contract employees.

All employees are expected to read and understand this handbook upon joining the company. Failure to comply with any policy herein may result in disciplinary action, up to and including termination of employment.

This handbook supersedes all previous versions of the employee policy manual. Any amendments will be communicated through official company channels and staff are required to acknowledge receipt of updates within 14 calendar days.

The policies contained in this document have been developed in consultation with legal counsel, the HR department, and senior management. They are reviewed annually and updated as necessary to reflect changes in legislation and best practice.

2. Remote Work Policy

Employees are permitted to work remotely up to 3 days per week, subject to line manager approval. Remote work arrangements must be documented using the Remote Work Agreement Form (HR-007) and renewed every 6 months.

All remote work must be performed from a secure, private location within the United Kingdom. Working from public spaces such as cafes, libraries, or co-working spaces on sensitive data is not permitted without prior authorisation from the IT Security team.

Employees working remotely must be available during core business hours (09:00-17:00 GMT) and must respond to communications within 30 minutes during these hours. Flexible scheduling outside core hours requires written approval from the department head.

Remote workers must use company-provided equipment and connect through the corporate VPN at all times. Use of personal devices for work purposes is governed by the BYOD policy (Section 13).

The company reserves the right to revoke remote work privileges with 5 working days notice if performance targets are not met or if security requirements are breached.

Remote workers are responsible for ensuring their home workspace meets health and safety requirements as outlined in the DSE (Display Screen Equipment) assessment policy. The company will provide ergonomic equipment upon request.

3. Data Security and Classification Policy

All company data must be classified according to the four-tier classification scheme: PUBLIC, INTERNAL, CONFIDENTIAL, and RESTRICTED. Data owners are responsible for assigning the correct classification level upon creation.

PUBLIC data may be freely shared outside the organisation. Examples include marketing materials, press releases, and published research papers.

INTERNAL data is for company-wide use and should not be shared externally without approval. Examples include internal memos, meeting minutes, organisational charts, and non-sensitive operational data.

CONFIDENTIAL data requires explicit authorisation for access and must be encrypted in transit and at rest. Examples include employee personal data, financial reports, customer lists, salary information, and strategic plans.

RESTRICTED data is the highest classification level and is limited to named individuals with a documented need-to-know. Examples include board-level discussions, M&A documentation, and security audit reports. RESTRICTED data must be stored only on approved encrypted systems.

Sharing of CONFIDENTIAL or RESTRICTED data externally requires written approval from the data owner and the Chief Information Security Officer. All external data transfers must use approved encrypted channels.

Data classification labels must be included in document headers and footers. Electronic files must include the classification in the filename suffix (e.g., report_Q4_CONFIDENTIAL.pdf).

Misclassification of data, whether intentional or negligent, constitutes a policy violation and will be investigated by the Data Governance team.

4. Password and Authentication Policy

All employees must use strong passwords for all company systems. Passwords must meet the following minimum requirements: at least 8 characters in length, containing at least one uppercase letter, one lowercase letter, one number, and one special character.

Passwords must be changed every 90 days. The system will enforce this automatically by prompting users 14 days before expiration. Employees who fail to change their password by the deadline will be locked out until IT Support resets their credentials.

Password reuse is prohibited for the last 12 passwords. Common passwords, dictionary words, and passwords containing the user's name or employee ID are blocked by the password policy engine.

Multi-factor authentication (MFA) is mandatory for all remote access, VPN connections, and access to CONFIDENTIAL or RESTRICTED systems. MFA tokens must be registered with IT Security before first use.

Sharing passwords with colleagues, contractors, or third parties is strictly prohibited, regardless of seniority or business justification. Each user account is tied to a single individual for audit purposes.

After 5 consecutive failed login attempts, the account will be locked for 30 minutes. After 10 consecutive failures within 24 hours, the account is permanently locked and requires IT Security intervention.

Employees must not write passwords on paper, sticky notes, or store them in unencrypted digital files. Use of the company-approved password manager (currently LastPass Enterprise) is mandatory.

5. Access Control and Authorisation

Access to CONFIDENTIAL and RESTRICTED systems is granted on a need-to-know basis, approved by the data owner and verified by IT Security. All access requests must be submitted via the Access Request Portal (ITS-003).

Access privileges are reviewed quarterly by the Access Review Board. Unused accounts (no login for 60 days) are automatically disabled. Accounts of departing employees are suspended on their last working day and deleted after 90 days.

Privileged accounts (administrator, root, service accounts) require additional controls including enhanced logging, session recording, and bi-annual access recertification. Privileged access must not be used for routine tasks.

External contractors and consultants are granted temporary access with a maximum duration of 90 days. Extensions require re-approval from the sponsoring department and IT Security.

Third-party access to company systems must be governed by a signed Non-Disclosure Agreement (NDA) and a Data Processing Agreement (DPA) where applicable.

Segregation of duties must be maintained: no single individual should have end-to-end control over a critical process without compensating controls. IT Security conducts annual SoD reviews.

6. Incident Response and Data Breach Procedures

All suspected security incidents must be reported to the Security Operations Centre (SOC) within 1 hour of discovery via email (soc@company.com) or the incident hotline (ext. 9999). Failure to report promptly is itself a policy violation.

The Incident Response Team (IRT) will triage all reported incidents within 4 hours and classify them as P1 (Critical), P2 (High), P3 (Medium), or P4 (Low) based on impact and scope.

P1 incidents (confirmed data breach, ransomware, system compromise) trigger the Major Incident Protocol: automatic escalation to the CISO, legal counsel, and the board. External communication is managed exclusively by the Communications team.

All P1 and P2 incidents require a Root Cause Analysis (RCA) report within 10 working days. The RCA must identify contributing factors, remediation steps, and preventive measures. Lessons learned are shared anonymously at the monthly Security Forum.

In the event of a personal data breach, the Data Protection Officer (DPO) must be notified immediately. The DPO will determine whether notification to the ICO (Information Commissioner's Office) is required within the statutory 72-hour window.

All employees must cooperate fully with incident investigations. Attempting to conceal, minimise, or delay reporting of a security incident will be treated as gross misconduct.

Incident logs are retained for 7 years for audit and regulatory compliance purposes.

7. Training and Awareness Requirements

All employees must complete mandatory security awareness training annually. New starters must complete the training within 30 days of joining. The training covers phishing recognition, data handling, password hygiene, and incident reporting.

Department heads are responsible for ensuring 100% completion rates within their teams. Completion status is tracked via the Learning Management System (LMS) and reported to the Security Committee quarterly.

Employees handling CONFIDENTIAL or RESTRICTED data must complete enhanced data protection training, including GDPR fundamentals and sector-specific compliance requirements.

Phishing simulation exercises are conducted monthly. Employees who fail two consecutive simulations are required to attend a mandatory 2-hour remedial workshop facilitated by IT Security.

Training content is updated annually by the Security Awareness team in collaboration with HR. Feedback from previous programmes and emerging threat intelligence inform content revisions.

Managers are required to complete an additional leadership security module covering their responsibilities for team compliance, access review, and incident escalation.

8. Acceptable Use of IT Resources

Company IT resources, including email, internet, software, and hardware, are provided for business purposes. Limited personal use is permitted provided it does not interfere with work duties, consume excessive bandwidth, or create security risks.

Installation of unauthorised software on company devices is prohibited. All software must be deployed through the company software catalogue, managed by the IT Service Desk.

USB storage devices may be used only with prior approval from IT Security and must be encrypted using company-approved encryption tools. Unencrypted USB devices are blocked by endpoint protection software.

Company email must not be used for personal financial transactions, political campaigning, religious solicitation, or distribution of offensive material. All email is subject to monitoring and archiving for compliance purposes.

Internet browsing is filtered by category. Access to known malicious sites, gambling platforms, adult content, and anonymous proxy services is blocked. Employees may request category exceptions through the IT Service Desk with business justification.

Circumventing security controls, including proxy bypass, VPN tunnelling to external services, or disabling endpoint protection, constitutes a serious policy violation.

Employees must immediately report any suspicious emails, attachments, or links to the SOC. If in doubt, do not click -- forward the message to phishing@company.com.

Company-provided mobile devices must be enrolled in the Mobile Device Management (MDM) solution. Remote wipe capability is enabled on all managed devices.

9. Physical Security

All office locations must maintain appropriate physical security controls including CCTV, access badge systems, and reception staffing during business hours.

Employee badges must be worn visibly at all times within company premises. Tailgating -- allowing unauthorised individuals to enter through controlled doors -- is prohibited. Report tailgating incidents to Facilities immediately.

The server room and data centre areas are classified as Restricted Zones. Access is limited to authorised IT Operations staff and requires both badge access and biometric verification.

Visitors to the office must sign in at reception, receive a visitor badge, and be escorted by their host at all times. Visitors must never be left unattended in any area. Visitor badges must be returned upon departure.

Visitors are never permitted in Restricted Zones (server rooms, data centres, security operations centre) under any circumstances, regardless of the visitor's seniority or purpose of visit.

Clean desk policy is mandatory in all open-plan areas. At the end of each working day, employees must: clear all documents from desks, lock filing cabinets, lock computer screens, and secure any removable media in locked storage.

Sensitive documents must be disposed of using cross-cut shredders provided on each floor. Regular waste bins must not be used for any documents containing company data.

Building access outside normal business hours (07:00-20:00) requires pre-authorisation from the department head and must be logged with Facilities.

10. Record Retention and Disposal

Company records must be retained in accordance with the Record Retention Schedule published by the Legal department. The retention schedule specifies minimum and maximum retention periods by document category.

Financial records: minimum 7 years from the end of the financial year. Employee personnel records: minimum 6 years after employment ends. Contracts: 6 years after expiry. Board minutes: indefinite retention.

Health and safety records, including accident reports and risk assessments, must be retained for 40 years from the date of the event.

Electronic records must be stored in approved document management systems with appropriate access controls and audit trails. Local storage of records on desktop computers or personal drives is not permitted for compliance-critical documents.

When the retention period expires, records must be disposed of securely. Paper records are shredded by the approved disposal contractor. Electronic records are deleted using certified data sanitisation tools that meet DoD 5220.22-M standards.

Ad hoc deletion of records outside the retention schedule is prohibited unless authorised by the Legal department. In the event of litigation or regulatory investigation, a legal hold may be placed to suspend normal disposal.

All destruction activities must be logged, including: document type, classification, volume, method of destruction, date, and the name of the responsible employee.

11. Cloud Services and Storage

Only cloud storage services approved by the IT department may be used for company data. The current approved services are Microsoft 365 (SharePoint, OneDrive), the corporate AWS tenancy, and Confluence for documentation.

Use of personal cloud storage services (Google Drive, Dropbox, iCloud, etc.) for company data is strictly prohibited, regardless of the classification level.

All data stored in cloud services must comply with the Data Classification Policy (Section 3). RESTRICTED data may only be stored in the dedicated encrypted zone within the corporate AWS tenancy.

Cloud services must be configured by IT Operations in accordance with security baselines. Self-provisioning of cloud resources by business users is not permitted without IT Security approval.

Backup and disaster recovery for cloud-hosted data is managed by IT Operations. Business-critical data is backed up daily with 30-day retention. Recovery Point Objective (RPO): 4 hours. Recovery Time Objective (RTO): 8 hours.

Cloud provider selection and onboarding requires a Security Assessment conducted by IT Security, covering: data residency, encryption, access controls, certifications (SOC 2, ISO 27001), and incident notification commitments.

12. Compliance and Consequences

All employees are expected to comply with the policies in this handbook. Ignorance of a policy is not an acceptable defence -- employees are responsible for reading and understanding all relevant policies.

Policy violations will be investigated by the relevant department in collaboration with HR and, where appropriate, Legal. Investigations will follow the Disciplinary Procedure outlined in the Employee Handbook.

Minor violations (first occurrence, low impact, no malicious intent) will typically result in a verbal warning and mandatory refresher training.

Moderate violations (repeat offences, negligent data handling, failure to follow procedures) may result in a written warning, temporary access restrictions, and enhanced monitoring.

Serious violations (intentional data theft, deliberate security bypass, harassment, fraud) will result in immediate suspension pending investigation. Confirmed serious violations may lead to summary dismissal and, where applicable, criminal referral.

Managers are responsible for enforcing policy compliance within their teams. Failure to address known violations by direct reports may itself constitute a policy violation.

An annual compliance audit is conducted by Internal Audit. Departments with significant non-compliance findings receive enhanced oversight and must submit remediation plans within 30 days.

The Compliance Committee, chaired by the Chief Compliance Officer, reviews policy effectiveness quarterly and recommends amendments based on audit findings, incident trends, and regulatory changes.

13. Bring Your Own Device (BYOD) Policy

Employees may use personal devices (smartphones, tablets, laptops) for work purposes subject to the conditions in this section. BYOD enrolment requires completion of the BYOD Agreement Form (IT-012) and device registration with IT Security.

All BYOD devices must be enrolled in the company Mobile Device Management (MDM) solution. MDM enables remote data wipe of company data containers without affecting personal data.

BYOD devices must meet minimum security requirements: current operating system version (within 2 major releases), device encryption enabled, screen lock with PIN/biometric, no jailbreaking or rooting.

Company data on BYOD devices is segregated in a secure container managed by the MDM solution. Personal apps cannot access data within the secure container.

The company reserves the right to remotely wipe the secure container if the device is lost, stolen, or if the employee leaves the company. Personal data outside the container is not affected.

BYOD devices must not be used to store RESTRICTED data under any circumstances. CONFIDENTIAL data may only be accessed (not downloaded) through the secure container.

Employees are responsible for the physical security of their personal devices. Lost or stolen devices must be reported to IT Security within 2 hours.

14. Travel and International Working Policy

Employees travelling internationally on company business must comply with additional security requirements. Travel to high-risk countries (list maintained by IT Security) requires pre-approval from the CISO.

A clean/loaner device must be used for travel to high-risk countries. Employees must not take their primary work device. Loaner devices are available from IT Security with 5 working days notice.

All data on travel devices must be encrypted with full-disk encryption. Sensitive data should be accessed via cloud services rather than stored locally on the device.

Public Wi-Fi networks must not be used for any company business. The corporate VPN must be active at all times when using hotel or conference Wi-Fi. Mobile hotspot is the preferred connection method.

Upon return from high-risk travel, loaner devices must be returned to IT Security for forensic inspection before being reissued. Any personal devices used during travel should be submitted for voluntary scanning.

Border control access to devices: if authorities request to inspect device contents, employees should comply but report the inspection to the Legal team and IT Security immediately upon return.

Employees must avoid discussing CONFIDENTIAL or RESTRICTED information in public settings (hotel lobbies, airports, restaurants) where conversations could be overheard.

15. Software Development and Change Management

All software changes to production systems must follow the Change Management process defined in ITIL Change Management Procedure (ITSM-005).

Standard changes (pre-approved, low-risk) can proceed through the automated deployment pipeline. Normal changes require a Change Request (CR) approved by the Change Advisory Board (CAB) at their weekly meeting.

Emergency changes bypass the normal CAB process but require retrospective approval within 48 hours. The Emergency Change Manager (on-call IT Operations lead) must authorise all emergency changes before implementation.

All code changes must undergo peer review before merging. The minimum review requirement is one independent reviewer for standard changes and two reviewers for changes affecting security-sensitive components.

Deployment to production occurs only during approved maintenance windows (Tuesdays and Thursdays, 22:00-02:00 GMT) unless an emergency change is authorised. Deployments must include a rollback plan.

Security-sensitive code changes (authentication, authorisation, encryption, data handling) require additional review by a member of the Security Engineering team before approval.

All changes are tracked in the ITSM tool with full audit trail: requester, approver(s), implementation date, test results, and post-deployment verification.

16. Anti-Bribery and Corruption Policy

The company has a zero-tolerance policy towards bribery and corruption in all its forms. This policy applies to all employees, directors, contractors, and agents acting on behalf of the company.

Employees must not offer, promise, give, request, or accept any bribe, whether in cash, gifts, hospitality, or other inducements, in connection with company business.

Gifts and hospitality may be given or received only if they are reasonable, proportionate, and given openly. All gifts or hospitality with a value exceeding 50 GBP must be declared in the Gifts and Hospitality Register and approved by the Line Manager and Compliance team.

Facilitation payments -- small payments to officials to speed up routine processes -- are prohibited regardless of local custom or practice. Any request for such a payment must be reported to the Legal team.

Due diligence must be conducted on all third-party partners, agents, and intermediaries before engagement. Enhanced due diligence is required for partners in countries with a Corruption Perception Index score below 50.

Employees who suspect bribery or corruption should report their concerns through the confidential whistleblowing hotline (0800-ETHICS) or to the Ethics Committee. Reports can be made anonymously. The company prohibits retaliation against whistleblowers.

17. Environmental and Sustainability Policy

The company is committed to minimising its environmental impact and operating sustainably. This policy sets out the environmental standards expected of all employees and departments.

All offices must participate in the company recycling programme, separating waste into general, paper, plastics, and electronic waste streams. Electronic waste must be disposed of through the approved WEEE disposal contractor.

Energy conservation measures include: automatic light sensors in meeting rooms and corridors, default screen timeout of 5 minutes on all company devices, and heating/cooling set to 20-22 degrees Celsius during business hours.

Business travel should be minimised where video conferencing is a viable alternative. When travel is necessary, rail transport is preferred over air travel for domestic journeys under 300 miles.

Each department must appoint a Sustainability Champion responsible for promoting environmental awareness and tracking departmental energy and waste metrics.

An annual Environmental Impact Report is published by the Facilities team, covering carbon emissions, waste volumes, and progress against sustainability targets.