LOOPOL SAMPLE

Construction Data Protection Pack

A connected set of data protection documents for construction companies and contractors, ready to adapt to your business.

What is included

- Privacy Policy
- Appropriate Policy Document
- Data Deletion and Destruction Protocol
- Complaints and Requests Handling Protocols
- Electronic Dispute and Access Systems
- Database Verification Protocols
- Site Surveillance and Vehicle Dashcam Policy
- Information Security Policies (SME and Enterprise alternatives)

SAMPLE

This is a watermarked sample showing the structure and drafting style of the pack. Placeholders such as [Your company's name] are completed for you when you buy, and every document is yours to adapt.

Buyers receive the full, complete versions of all documents. To make an enquiry or buy the pack, visit the Loopol store.

Privacy Policy

Extract from the pack. The full document continues after this sample.

[Your company's name] is committed to protecting your privacy. This Privacy Policy describes how we collect, use, disclose, and safeguard your personal data when you visit our website and use our services.

We are typically the data controller for the personal data we collect regarding our own staff, direct clients and suppliers. However, where we process personal data on behalf of an upstream client or employer, we act as a data processor on their documented instructions.

Information we collect

We collect the following types of information:

a. Personal information

Name, home and site/postal address, telephone numbers, email address, date of birth and emergency contact details.
Email address and communication history
Payment, banking, and tax identifiers (including National Insurance numbers for sole traders, UTRs, and CIS numbers for sub-contractors).

Employment records, trade qualifications, CSCS/machine tickets and proof of right-to-work
Health and injury reports, sickness absence records and occupational health details
Occupational health recommendations, disability disclosures, workplace reasonable adjustments, medical fit-to-work certificates, statutory accident reports (RIDDOR) and certified results of drug and alcohol screening tests.
Contact details, access notes, and appointment schedules for residents, tenants, and end users on occupied residential refurbishment or maintenance projects.
Any other information you voluntarily provide to us

b. Technical, surveillance and access information

The following information is personal data where it relates to an identified or identifiable individual. It must be handled under the same data protection safeguards as other personal data. Biometric data processed to uniquely identify an individual is special category personal data and requires an appropriate Article 6 lawful basis and Article 9 condition.

IP address, browser type and version
Device information and website usage data (pages visited, time spent)
Cookies and tracking technologies
Fixed-perimeter site security CCTV, time-lapse build footage, company vehicle dashcam recordings, plant telemetry and fleet GPS tracking logs.
Digital turnstile sign-in timestamps and biometric access templates (where automated facial or fingerprint recognition is deployed to manage site safety, access control, and CDM emergency muster rolls).

SAMPLE

How we use your personal data and our lawful bases

Data category	Purpose	Lawful basis
Contact and communication data	To respond to inquiries and customer service requests.	Contract
Website usage and technical data	To personalise users' experience when using our website.	Legitimate interest (of maximising the user experience for our customers and potential customers)
Accounting and financial records	Accounting and book-keeping.	Contract
Auditing	Conducting internal data audits to ensure compliance with data protection laws and our policies.	Legitimate interest (of ensuring our business is in good order) Contract Legal obligation
Business administration and operation	To ensure the compliant and efficient running of the business.	Contract Legitimate interest (of ensuring our business is properly managed)
Client awareness	To understand how clients and potential clients became aware of our services.	Legitimate interest (of ensuring marketing and business development is properly targeted and effective)

The table continues in the full document, covering a further fifteen data categories including HR, sub-contractor, project and recruitment data.

SAMPLE

Appropriate Policy Document

Extract from the pack. The full document continues after this sample.

[Your company's name]: APPROPRIATE POLICY DOCUMENT (APD)

For the processing of special category and criminal offence data, pursuant to Schedule 1, Part 4 of the Data Protection Act 2018

1. Purpose and scope

This Appropriate Policy Document (APD) explains how [your company's name] handles special category personal data and criminal offence data in compliance with the UK GDPR and the Data Protection Act 2018 (DPA 2018). Under Schedule 1 of the DPA 2018, certain conditions for processing sensitive data, specifically relating to employment, health, safety and substantial public interest, require the controller to have an operational policy in place which demonstrates compliance with the core data protection principles.

This document should be read alongside [your company's name]'s privacy policy, data retention schedules and internal data protection governance framework.

2. Categories of sensitive data

[Your company's name] processes the following categories of sensitive information:

Data concerning health
Sickness absence records, occupational health assessments, medical fit-to-work certificates, accident reports (RIDDOR), workplace and recruitment reasonable adjustment information and drug and alcohol screening tests.
Criminal offence data
Data relating to criminal record checks, right-to-work verifications and compliance vetting under the Construction Industry Scheme (CIS).

3. Conditions for processing

We rely on the following legal bases under Article 9 and Article 10 of the UK GDPR, supported by Schedule 1 of the DPA 2018:

Employment, social security and social protection (Article 9(2)(b) and Article 10)

Supported by Schedule 1, Part 1, Paragraph 1 of the DPA 2018
Necessary for carrying out our legal obligations and specific rights as an employer in the construction sector.
Occupational health and assessment of working capacity (Article 9(2)(h))

Supported by Schedule 1, Part 1, Paragraph 2 of the DPA 2018.
Necessary for preventative medicine, medical diagnosis and assessing the working capacity of site personnel and employees.
Statutory health and safety duties (Article 9(2)(b) and (h))
Ensuring a safe working environment, managing plant safety and executing mandatory pre-

SAMPLE

commencement or random drug and alcohol screenings for safety-critical roles.

4. Procedures for compliance with the data protection principles

[Your company's name] applies technical and organisational safeguards to ensure full adherence to the principles set out in Article 5 of the UK GDPR.

Lawfulness, fairness and transparency

All processing of sensitive data is tied to clear statutory safety duties, employment contracts or regulatory obligations, with transparent disclosures provided via our privacy policy.

Purpose limitation

Health, safety and screening data are collected to manage site safety, assess fitness to work, fulfil legal obligations and defend potential employment or personal injury claims. Data is not repurposed for unrelated commercial objectives.

Data minimisation

We collect only the information strictly necessary to ensure operational safety and legal compliance. We do not collect and/or delete as applicable, unnecessary medical details or irrelevant background disclosures.

Accuracy

Personnel files, fitness certificates and screening outcomes are kept up to date. Staff and sub-contractors may request rectification of factual inaccuracies at any time.

Storage limitation

Sensitive records are retained only for the minimum time required to meet the purpose, including where that is set down by statute. These retention periods are strictly adhered to.

Integrity and confidentiality (security)

Physical health files are stored in locked cabinets or access-restricted HR sub-folders. Electronic records are protected by strong encryption and role-based access controls restricted on a need-to-know basis.

SAMPLE

Data Deletion and Destruction Protocol

Extract from the pack. The full document continues after this sample.

[Your company's name]: DATA DELETION AND DESTRUCTION PROTOCOL

1. Purpose and scope

This protocol governs the secure, compliant, and permanent destruction of personal data held by [your company's name] across all physical and electronic formats. It ensures that data is neither retained longer than specified in our Data Retention and Document Destruction Schedule nor destroyed prematurely in violation of statutory limitation periods or active legal holds.

2. Authorisation and governance

Execution authority

Routine scheduled purging of expired data is coordinated by the data protection lead or designated office manager in alignment with our retention periods.

Legal overrides

Any deviation from standard deletion schedules (such as placing a file under a litigation hold or refusing an erasure request based on the Limitation Act 1980 or HMRC rules) must be authorised and signed off in writing by a company director or the DPO.

3. Deletion categories and methods

Electronic files and cloud storage

Digital files must be permanently deleted from active directories, project folders and cloud storage accounts, followed by emptying local trash or recycle bins. Where records are stored within third-party cloud platforms or software systems, administrators must use the standard deletion, archive removal or purging functions built into those platforms.

Physical paper records

Physical documents must be cross-cut shredded on-site using a standard office shredder, or placed into locked confidential waste bins managed by an external shredding contractor.

If using an external shredding company, always obtain and file their Certificate of Destruction. For internal office shredding, a staff member must log the date, category of files shredded, and their initials in your data management records.

4. Special category and criminal offence data

Special category records (such as health surveillance, fit notes and drug screening results) and records relating to criminal convictions, offences or related security measures require heightened security during disposal. CIS vetting and right-to-work documentation are not criminal offence data merely because they are compliance records; their classification depends on the information they contain.

Physical records

When gathering expired medical files, fit notes or vetting documents for destruction, they must not be left unattended on desks or in site cabins. They must be moved directly from locked cabinets or restricted HR folders directly into a locked confidential waste bin or cross-cut shredder.

Digital records

When purging expired sensitive files from digital systems, administrators must ensure that files are

SAMPLE

permanently deleted and that trash bins are immediately emptied, to avoid them being temporarily moved to accessible shared folders or unencrypted local desktop folders during the deletion process.

COMPLAINTS AND REQUESTS HANDLING PROTOCOLS
[Your company's name]: Subject Access Request Process

The data subject's right

Individuals have the right to access and receive a copy of the personal data, and any supplementary information, [Your company's name] holds about them. This allows them to understand how [Your company's name] processes their data, and to check that [Your company's name]'s processing is lawful.

SAMPLE

Complaints and Requests Handling Protocols

Extract from the pack. The full document continues after this sample.

[Your company's name]: Subject Access Request Process

The data subject's right

Individuals have the right to access and receive a copy of the personal data, and any supplementary information, [Your company's name] holds about them. This allows them to understand how [Your company's name] processes their data, and to check that [Your company's name]'s processing is lawful.

Recognising a Subject Access Request/Subject Access Request

The request, often referred to as a 'SAR', can be made verbally, in writing or by social media.
All employees must be alert to the possibility that a request may have been made.
Sub-contractors and Agency Workers: The right of subject access applies to all individuals whose personal data [Your company's name] holds. This includes direct PAYE staff, CIS sub-contractors, self-employed tradespeople, agency workers and site visitors. Staff must treat requests from non-PAYE site personnel with the same process and urgency as direct employees.
No specific form of words is required, and there is no need for the request to reference data protection or the UK GDPR. Examples could include:

'I would like to see what information you hold about me'
'I want to see all information relating to the applications I've made'
'What personal data do you hold about me?'
'I would like copies of my personnel records and anything relevant to my employment'

Verifying identity

[Your company's name] must satisfy itself that it knows the identity of the data subject (or the person on whose behalf the request is being made and the individual making the request if they are not the same). If [Your company's name] is unsure, it should promptly request ID documents.
The DPO/data protection lead, should ask the person who received the request if they are confident that it was made by the data subject. For example, if it came from the usual correspondence email, or the individual was personally recognisable on the phone.
The DPO/data protection lead should confirm with the employee who received the request that they are satisfied as to the requesting party's identity. If not, the DPO/data protection lead should use the data subject's usual correspondence address to request confirmation of their ID.
For verbal requests, the email requesting confirmation in writing should also include an ID confirmation request.
If a request is made by social media, the data subject is contacted by phone to confirm that the request was from them. (The risk is a compromised social media account, which may also imply a compromised email.) A note should be made of this. An email should be sent requesting confirmation as to scope.

Requests by third parties

It is possible for someone to make an access request on someone else's behalf, for example a friend,

SAMPLE

relative or solicitor.
[Your company's name] must satisfy itself that the third party has authority to make the request, by asking for evidence, which must be assessed on a case-by-case basis.

The DPO/data protection lead sends an email to the third party requesting such confirmation. If the third party makes the request verbally or by social media, [Your company's name] should ask for their email address in order to do this.
If the third party makes the request by post and includes their email in that correspondence, [Your company's name] should ask for confirmation by email. Otherwise [Your company's name] should make the request by post.

Charging a fee

Generally, [Your company's name] can't charge a fee for dealing with the request. However, there are exceptions. A reasonable administration fee may be charged when the request is manifestly unfounded or excessive, or if an individual requests further copies of their data.
The charge can take into account:

The cost of assessing whether [Your company's name] is processing the information.
The cost of locating, retrieving and extracting the information.
The cost of providing copies.
The cost of communicating with the data subject (or third-party requesting individual).
The cost of photocopying, printing, postage and estimated hourly staff costs.

There mustn't be any double-charging.
Where a fee is due and has been requested, [Your company's name] doesn't have to comply with the request until it has received the fee.
The fee should be requested within one calendar month.
If the fee is not received within one calendar month the request is closed, and a record made of why this is reasonable.

Timeframe for responding and recording of correspondence and actions

[Your company's name] should respond to any request as soon as possible, but in any event within one calendar month of the date of receipt.
If there is uncertainty about the identity of the data subject (or the requesting individual if different), the one-month deadline begins after [Your company's name] has received confirmation of the person's identity. Any request for ID confirmation must be made without delay after the request is received.
If the scope of the request is unclear or seems very broad, [Your company's name] can request confirmation of exactly which data is required. The one-month deadline does not begin until that confirmation is received.
If a request is particularly complex, or multiple requests are received from the same individual, the deadline may be extended for up to two months.
A confirmation email should be sent to the requesting individual (or to the data subject if that is deemed appropriate in the case of third-party requests), by the end of the first working day after receipt of the request. Ideally, this should be automated.
The date of receipt of the request must be recorded.

SAMPLE

The date of the confirmatory email must be recorded.
The date of receipt of any additional information requested must be recorded.
Any outstanding information which delays or prevents dealing with the request must be recorded.
Any extension to the deadline is to be recorded.
Any decision as to whether to comply with the request, refuse the request, charge a fee, or provide restricted information only must be recorded, with justifications, and signed by a director or a designated member of senior management.
The form in which the data is to be provided must be recorded.
The date on which the information is provided must be recorded.
Any subsequent correspondence with the data subject (or other requesting individual) must be recorded.
All recorded information must be kept in a secured, dedicated file.
Summarised details of the request are to be added to the data disputes and rights register.

Requesting clarification of scope

Unless the request is clearly limited and specifies exactly what the individual wants us to provide, we ask in the initial confirmation email for the person to indicate in writing the scope of their request.
The response deadline begins once we have received this information.
[Your company's name] should include any such request for clarification in its initial communication with the individual (i.e. sent by the end of the first working day after receipt of the request.)
[Your company's name] should provide supplemental information as soon as possible, and irrespective of scope.

SAMPLE

Electronic Dispute and Access Systems

Extract from the pack. The full document continues after this sample.

Safeguards and compliant electronic complaint-handling mechanisms.

[Your company's name]: DATA DISPUTES AND RIGHTS REGISTER
Restricted access. Directors and Data Protection Team Only. Store securely with password protection.

Description/dropdown options

Register field	What to enter
Ref no.	Unique [Your company's name]-given ID
Date received	Date the email arrived/complaints or request made
Complainant's name	Full name of the data subject
Category	[Client] [Sub-contractor] [Employee] [Public]
Contact details	Email address or phone number
Request type	[Privacy Complaint] [SAR] [Erasure] [Rectification] [Restriction] [Objection]
Target deadline	1 calendar month
Assigned Lead	Director or office manager handling the file
Summary of request	Brief details
Action taken and overrides applied	Actions taken
Status	[Received] [Under Investigation] [Response Sent] [Closed] [Escalated to ICO]
Completion date	Actual date the final written response was issued

SAMPLE

Strategy 1. Deadline for actioning request or investigating a complaint.

You have a deadline for investigation of a complaint or executing a request in full, of 1 calendar month.

Strategy 2. Automate immediate acknowledgments

For the complaint-handling requirements under the Data (Use and Access) Act, the law requires acknowledging receipt within 30 days. The ICO has confirmed that an automated auto-responder email fulfills this requirement. When an individual submits a request or complaint the system sends an automated receipt email:
'Thank you for contacting us regarding your personal data. Your request has been logged under reference [REF-NUMBER]. We are currently reviewing your details and will be in touch with an update within 28 days.'

2. Worked examples

Database Verification Protocols

Extract from the pack. The full document continues after this sample.

Internal workflows for verifying regulatory, corporate and land registers.

[Your company's name]: DATABASE VERIFICATION PROTOCOLS

1. Overview

This protocol sets out the mandatory procedures used by [Your company's name] to verify third-party identities, corporate records, tax registration statuses and property ownership, prior to entering into contracts, granting site access or making payments.

Under the UK GDPR, Data Protection Act 2018, and the Data Use and Access Act 2025, personal data collected during verification checks must be handled lawfully, securely and only for the purpose it was collected.

2. Companies House and Identity Verification

Scope

Applies to all limited company sub-contractors, corporate clients, material suppliers and equipment hire vendors.

Verification portal

Companies House online

Verification workflow

Step 1

Search the company name in the Companies House register before signing contracts.

Step 2

Confirm the current status is listed as 'active'. Do not enter into agreements with dissolved, liquidated or struck-off entities.

Step 3

Verify that the registered office address matches the address given on invoices and commercial proposals.

Step 4

Cross-reference the names of active company directors listed on Companies House against the individuals signing commercial contracts or vendor declarations.

Data retention

Retain a digital export or PDF copy of the Companies House record in the vendor or project file for the duration of the agreement plus six years (for accounting and audit purposes).

3. HMRC CIS and VAT register checks

Scope

Applies to all sole trader and corporate sub-contractors subject to CIS and all VAT-registered suppliers.

Verification portals

HMRC CIS online service

GOV.UK VAT number check

CIS verification workflow

Step 1

Collect the sub-contractor's full legal name, UTR, NI Number for sole traders or Company Registration

SAMPLE

Number for limited companies/LLPs.
Step 2
Input details into the HMRC CIS portal to generate formal tax verification.
Step 3
Record the HMRC verification number and confirm the deduction rate (Gross Payment Status 0%, Standard Rate 20% or Higher Rate 30%) into the accounting ledger.
Step 4
Sub-contractors who have not been included on a [Your company's name] monthly CIS return within the current or previous two (2) tax years, must be re-verified through the portal before any further payments are cleared.

VAT verification workflow
Step 1
Input the supplier's 9-digit VAT number into the GOV.UK verification tool.
Step 2
Confirm the registered business name and address returned by the system match the vendor's invoice details exactly.
Step 3
Where the DRC for building and construction services applies, ensure supplier profiles are flagged in any accounting software to ensure zero VAT is applied to DRC invoices.

Data retention
CIS verification confirmations and VAT search results must be archived securely in the digital finance folder for six complete tax years to satisfy HMRC's statutory audit requirements.

SAMPLE

Site Surveillance and Vehicle Dashcam Policy

Extract from the pack. The full document continues after this sample.

Operational policy for on-site security surveillance, vehicle dashcams, and physical site information boards adhering to ICO public data guidelines.
[Your company's name]: SITE SURVEILLANCE AND VEHICLE DASHCAM POLICY

1. Purpose
This policy covers the use of vehicle dashcams in company vans and any temporary overnight security cameras used by [Your company's name]('[Short form of your company's name]') on residential projects. Under the UK GDPR, the Data Protection Act 2018 and the Data Use and Access Act 2025, video recorded in public, on client driveways or capturing identifiable people is personal data. This policy ensures that [Short form of your company's name] uses cameras legally, transparently and proportionately.
2. Vehicle dashcams (company vans and trucks)
Purpose
Where dashcams are fitted to [Short form of your company's name]'s vehicles it is solely for driver safety, road traffic accident evidence and insurance defence.
Placement
Cameras must be mounted high in the centre of the windscreen behind the rear-view mirror. They must not block the driver's view of the road.
In-cab audio
Internal cabin audio recording must be turned off by default to protect driver and passenger privacy.
Footage retention
Routine driving footage must be set to overwrite automatically on a rolling basis (for example, every 3 to 7 days).
Accident protocol
If a road collision or incident occurs, the relevant footage must be downloaded immediately and saved into a secure company incident file.
Social media ban
Dashcam footage must never be uploaded to social media. Footage may only be shared with insurance companies, the Police or legal advisers.

3. Temporary on-site security cameras
When used
[Short form of your company's name] may occasionally place temporary battery-powered security cameras or site alarms on residential sites overnight or over weekends to protect high-value materials, tools or heavy plant machinery.
Positioning
Cameras must be pointed strictly at [Short form of your company's name]'s materials, equipment or working area. They must never be directed at neighbouring windows, adjoining private gardens, or public pavements.
Audio recording
Continuous audio recording is strictly prohibited.
Retention
Site footage must be set to overwrite automatically within 30 days unless an active break-in, damage, or safety incident requires footage to be saved as evidence.

SAMPLE

4. Site notices

Whenever temporary security cameras are active on a site, a weatherproof warning sign must be attached to the main access gate or plant area.

Standard A4 weatherproof sign (yellow/black or blue/white)

ATTENTION: SITE SURVEILLANCE IN OPERATION

Cameras are operating on this site for the purposes of crime prevention, site security, and asset protection.

Data Controller: [Your company's name] [Your company's address]

Enquiries: [Your company's name contact details for the data protection lead or data protection officer (phone number and email if possible)]

Images are recorded and stored securely in accordance with the UK GDPR and the Data (Use and Access) Act 2025.

5. Managing CCTV footage and access

Security

Camera memory cards, cloud accounts and phone viewing applications must be password-protected and accessible only by company directors or site leads.

Requests to view footage

If a client or member of the public asks to see footage of themselves, [Short form of your company's name] must verify their identity and provide the clip within one month. Other individuals or non-relevant vehicle number plates visible in the clip must be blurred out before sharing.

INFORMATION SECURITY POLICIES (SME AND ENTERPRISE ALTERNATIVES)

[This policy is for smaller companies. Intake questions should include establishing which policy is more appropriate as a starting template.]

[Your company's name]: IT SECURITY AND ACCEPTABLE USE POLICY

SAMPLE

Information Security Policies (SME and Enterprise alternatives)

Extract from the pack. The full document continues after this sample.

[This policy is for smaller companies. Intake questions should include establishing which policy is more appropriate as a starting template.]
[Your company's name]: IT SECURITY AND ACCEPTABLE USE POLICY

1. Purpose and Scope
1.1 Objective
This policy establishes mandatory operational standards for the secure use, handling and governance of information technology assets, software platforms, mobile devices and data across all office, remote and site environments. Its primary objective is to protect [your company's name] systems, commercial confidential data and personal data from unauthorised access, loss, cyber-attack and regulatory breach under the UK GDPR, the Data Protection Act 2018 and the Computer Misuse Act 1990.
1.2 Scope

This policy applies to:
All employees, fixed-term staff and directors.
Site managers, project leads, quantity surveyors and foremen handling company or operative data on site.
Agency workers, self-employed sub-contractors, consultants, and third-party IT service providers granted access to company hardware, email systems, cloud networks or site management software.

Compliance with this policy is a condition of employment and a mandatory contractual term in commercial engagements.

2. Authentication, Passwords and Access Control
2.1 Password management

Passwords must consist of a minimum of twelve (12) characters and include a mixture of uppercase letters, lowercase letters, numbers and symbols, or follow a verified three-random-word passphrase structure.
Users must never reuse company passwords across personal accounts or third-party non-work applications.
Passwords must not be recorded in plain text, written on paper, stored on adhesive notes attached to screens or saved in unencrypted local documents.
Where applicable, users must use the company-approved password manager.

2.2 Multi-Factor Authentication

Multi-factor authentication is mandatory on all accounts accessing business email, cloud drives, accounting software, site administration platforms and remote management tools.
Users must not bypass, disable or attempt to reconfigure MFA protections without prior written sign-off from the DPO or designated privacy or IT lead (as the case may be).
MFA approval prompts received without an active login attempt must be denied immediately and reported as a potential security incident.

SAMPLE

2.3 Account confidentiality

User credentials are strictly individual. Sharing account logins, passwords or temporary verification tokens between colleagues or with third-party trades is strictly prohibited.
Access to databases, folders and platforms is granted on a need-to-know basis aligned with the user's operational role. Users must not attempt to access systems, restricted commercial tenders or HR/personnel folders for which they have not received formal authorisation.

3. Hardware, mobile devices and site security
3.1 Device screen locks and timeouts

All laptops, tablets and desktop computers must be configured to lock automatically after a maximum of five (5) minutes of user inactivity.
Users must manually lock their devices whenever stepping away from their desk, vehicle or site station, regardless of the duration.

3.2 Site and vehicle security
Construction sites, temporary site cabins and vehicles represent high-risk environments for hardware theft and unauthorised physical access. Operatives and site managers must enforce the following controls:
Site cabins
Site laptops, tablets, digital cameras, and mobile phones must never be left unattended in unlocked site cabins, welfare units or open desk spaces. When cabins are unoccupied, devices must be placed inside locked storage cabinets or taken off-site.
Vehicles
Company laptops, tablets, tools with telemetry data and physical site files must not be left visible in unattended vehicles. If equipment must be temporarily left in transit, it must be locked out of sight inside a secure boot or tool vault. Devices must never be left inside vehicles overnight.
Paper and physical records
Hard-copy site registers, induction logs, sub-contractor questionnaires, accident books and daywork sheets must be kept in locked filing cabinets or secure weatherproof site compliance folders. They must never be left exposed in public site areas or domestic driveways where clients, trades or visitors can inspect them.

3.3 Bring Your Own Device protocol
Where personnel use personal smartphones or tablets to access company email, messaging groups or site platforms:
The device must be protected by a mandatory PIN (minimum 6 digits), biometric lock or alphanumeric passcode.
The operating system must remain supported and updated with current vendor security patches.
The user agrees that upon termination of employment or engagement, or following the loss or theft of the device, [your company's name] reserves the right to enforce a remote wipe of all business data, corporate email and project folders.

4. Removable Media and Data Export Restrictions
4.1 Prohibition on unauthorised removable storage

SAMPLE

The connection and use of personal, unencrypted USB flash drives, memory sticks, external hard drives or SD cards to company hardware is strictly prohibited.
Users must not transfer project databases, estimating spreadsheets, employee records or sub-contractor compliance files to unencrypted external storage media.
Where external data export is required for engineering equipment or site surveying machinery, only company-issued, BitLocker/hardware-encrypted media may be used.

4.2 Cloud storage and personal email restrictions

Users are strictly forbidden from emailing [your company's name]'s spreadsheets, customer lists, resident contact logs or commercial agreements to personal email accounts for home working, printing or convenience.
[Your company's name]'s data must reside solely within company-sanctioned cloud infrastructure.
Uploading business files or customer details to personal cloud accounts constitutes a serious security breach.

5. Software Integrity, Artificial Intelligence and Network Controls
5.1 Authorised software and unofficial downloads

Users must only install and execute software, browser extensions and applications approved by [your company's name] management.

SAMPLE