Data Protection Policy

2023 version

This document has been submitted and approved by the HSE Building Safety Regulator.

BUILDING CONTROL SURVEYORS LTD

Registered Building Control Approver

DATA PROTECTION, INFORMATION SECURITY, CONFIDENTIALITY AND RECORDS MANAGEMENT POLICY

Document Reference: BCS-QMS-DP-01. Version 3 : 2 April 2023
ISO 9001:2015 Status: Controlled Document
Policy Owner: Managing Director / Quality Manager
Approved By: Directors of Building Control Surveyors Ltd, Warlies Park House, Teulon Wing, Horseshoe Hill, Upshire, Essex EN9 3SL.
Review Frequency: Annually, or earlier following legislative or regulatory change
Minimum Regulatory Record Retention: 15 years, subject to the longer periods specified within this policy
Applicable Legislation: UK GDPR, Data Protection Act 2018 and other applicable data protection legislation
Regulatory Framework: Building Act 1984; Building Safety Act 2022; Building Regulations 2010 (as amended); applicable RBCA legislation; Operational Standards Rules; applicable professional conduct requirements for RBCAs and Registered Building Inspectors
ISO 9001:2015: Clauses 4.4, 5.2, 7.2, 7.3, 7.5, 8.1, 9.1, 9.2 and 10.2, where applicable

---

1. Policy Statement

Building Control Surveyors Ltd ("BCS") recognises that information obtained, generated, processed and retained in the course of providing registered building control services is a valuable corporate, regulatory and evidential asset.

BCS shall protect such information against unauthorised access, disclosure, copying, alteration, deletion, loss, misuse or transmission.

Information held within BCS databases, network storage systems, document management systems, email systems, cloud services, backup facilities and other authorised information systems remains under the control of BCS and may only be accessed or used for legitimate and authorised business, regulatory, training, competence or employment purposes.

Access to BCS information is granted on the basis of need, role, competence and contractual authority. The ability technically to access information does not constitute authority to use, copy, print, download, transmit or disclose it.

No employee, Registered Building Inspector, consultant, contractor, trainee or other person working for or on behalf of BCS acquires any personal right to retrieve, retain, reproduce, transmit or use information merely because that person has been provided with access to a BCS system.

---

2. Purpose

The purpose of this policy is to establish controls for:

- protection of personal, commercial, technical and regulatory information;
- confidentiality of applicant, client, agent and dutyholder information;
- secure management of building control records;
- compliance with the UK GDPR and Data Protection Act 2018;
- compliance with applicable Operational Standards Rules;
- compliance with applicable professional conduct requirements for RBCAs and RBIs;
- control of documented information under ISO 9001:2015;
- secure retention and retrieval of regulatory evidence;
- use of project information for authorised staff training, supervision and competence evaluation;
- prevention of unauthorised extraction, copying or removal of company information; and
- secure retention and eventual disposal of information.

---

3. Scope

This policy applies to all directors, employees, Registered Building Inspectors, trainee inspectors, consultants, agency staff, contractors and other persons given access to BCS information.

It applies to information in any format, including:

3.1 Building control and project information

This includes:

- drawings and plans;
- specifications;
- structural calculations;

- design calculations;
- fire strategies;
- energy calculations;
- SAP/SBEM information;
- drainage information;
- technical reports;
- inspection records;
- site photographs and videos;
- geolocation information associated with inspections;
- correspondence;
- consultation responses;
- Initial Notices and statutory notices;
- certificates;
- declarations of compliance;
- contravention records;
- regulatory interventions;
- technical assessments;
- evidence relied upon by an RBI or BCS;
- professional judgements and decisions;
- records demonstrating the reasoning behind regulatory decisions; and
- any other material forming part of the regulatory project record.

3.2 Personal and client information

This includes:

- names;
- property and project addresses;
- postal addresses;
- email addresses;
- telephone and mobile telephone numbers;
- signatures;
- correspondence;
- contractual information;
- invoices and financial information;
- applicant, client, agent and dutyholder details; and
- any other information capable of identifying an individual.

3.3 Staff and competence information

This includes:

- employment records;
- training records;
- CPD records;
- competence assessments;
- supervision records;
- RBI registration information;
- performance and evaluation records;
- internal technical reviews;
- examination or assessment evidence;
- training exercises;
- records of mentoring;
- quality audits;
- competency portfolios; and
- project information lawfully used to demonstrate, assess or maintain competence.

---

4. Data Protection Principles

BCS shall process personal information in accordance with the principles of UK data protection law.

Personal information shall therefore be:

1. processed lawfully, fairly and transparently;
2. collected for specified and legitimate purposes;
3. adequate, relevant and limited to what is necessary;
4. accurate and, where necessary, kept up to date;
5. retained for no longer than is necessary, subject to statutory, regulatory, contractual, professional indemnity and evidential requirements;
6. protected by appropriate technical and organisational security measures; and
7. processed in a manner for which BCS can demonstrate accountability.

Nothing within this policy authorises the retention of personal information merely because BCS has the technical capacity to retain it.

---

5. Regulatory Building Control Records

BCS shall maintain accurate and up-to-date records sufficient to demonstrate the proper exercise of its building control functions.

Regulatory records shall include, where applicable, sufficient evidence to demonstrate:

- what information was submitted;
- what information was considered;
- which RBI considered the matter;
- the competence and registration status relevant to restricted activities and functions;
- inspections undertaken;
- evidence obtained;
- correspondence and consultation;
- matters raised with dutyholders;
- regulatory decisions made;
- professional judgements exercised;
- the reasoning supporting material decisions;
- interventions and contraventions;
- Initial Notice and Final Certificate processes; and
- other information necessary to establish an appropriate audit trail.

The regulatory file shall, so far as reasonably practicable, constitute the authoritative record of BCS's involvement with the project.

6. Retention

6.1 Building control records

BCS shall retain records relating to its building control functions for a minimum period of 15 years from completion of the work, or for a longer period where required by:

- legislation;
- applicable regulatory rules;
- the terms of BCS registration;
- professional indemnity insurance requirements;
- contractual obligations;
- litigation or anticipated litigation;
- an investigation;
- enforcement proceedings; or
- a formal legal hold.

Where another applicable regulatory requirement requires the retention period to run from an earlier date, including the date of instruction, BCS shall operate the retention period that produces the longer retention period.

6.2 Professional decisions and evidence

Evidence, instructions, advice, professional judgements and regulatory decisions shall be retained for not less than the applicable regulatory period and, where required, 15 years from the date of instruction or in accordance with applicable insurance requirements, whichever is longer.

6.3 Staff training and competence records

Records of learning, development, competence and CPD undertaken by persons working for BCS shall be retained for a minimum of 15 years where required by the applicable professional conduct requirements.

This may include appropriately controlled project information used as evidence of an individual's competence.

The termination of employment does not automatically require deletion of competence records where BCS has a lawful or regulatory basis for continuing to retain them.

6.4 Legal hold

Information shall not be destroyed where BCS knows or reasonably anticipates that it may be relevant to:

- litigation;
- a complaint;
- regulatory investigation;
- disciplinary proceedings;
- insurance notification;
- professional conduct proceedings;
- enforcement proceedings; or
- any other legal or regulatory process.

---

7. Access Control – "Need to Know" Principle

Access to information shall be limited to persons with a legitimate requirement to access it.

BCS shall apply role-based access controls where reasonably practicable.

Access rights shall be determined by:

- employment role;
- RBI class and competence;
- assigned projects;
- supervisory responsibilities;
- management responsibilities;
- contractual responsibilities; and
- regulatory requirements.

BCS reserves the right to restrict access to individual files, projects, folders, databases or categories of information.

Users must not attempt to circumvent access restrictions or obtain access to information outside their authorised responsibilities.

---

8. Retrieval, Viewing, Printing, Downloading and Transmission

Information held on BCS databases, network drives, servers, cloud storage, CRM systems and associated systems shall only be:

retrieved, searched, viewed, printed, copied, downloaded, photographed, screen-captured, exported, emailed, uploaded, transmitted or otherwise processed where the person doing so has an authorised business, contractual, regulatory or legal reason.

In particular:

8.1 Viewing

Information shall only be viewed where necessary for the performance of authorised duties.

8.2 Printing

Printing shall be minimised.

Where printing is necessary:

- documents must not be left unattended;
- documents must be stored securely;
- unnecessary copies must not be produced;
- confidential waste must be securely destroyed; and
- printed documents must not be removed from authorised premises except where required for authorised duties.

8.3 Downloading and copying

Project files shall not be copied to personal computers, privately owned devices, personal cloud storage, removable media or unauthorised systems.

8.4 Email and electronic transmission

Information shall only be transmitted:

- to authorised recipients;
- for legitimate business or regulatory purposes;
- using BCS-approved systems;
- with reasonable steps taken to verify the recipient; and
- with appropriate security measures having regard to the sensitivity of the information.

Particular care shall be exercised before transmitting information containing personal data, commercially sensitive information, security information, building plans or large collections of project data.

---

9. Confidentiality

Information obtained from an applicant, client, agent, dutyholder or other person in connection with building control work shall be treated as confidential.

It shall not be disclosed except where disclosure is:

- necessary for the authorised performance of BCS's functions;
- expressly authorised by the person entitled to authorise disclosure;
- required or authorised by law;
- necessary in connection with legal proceedings;
- required by the Building Safety Regulator, local authority, fire and rescue authority or other competent regulator;
- necessary for reporting suspected crime or a breach of building control requirements; or
- otherwise permitted under the applicable professional conduct requirements.

Contractual confidentiality obligations continue following termination of employment or engagement.

---

10. Use of Project Data for Staff Training, Supervision and Competence Evaluation

BCS recognises that Registered Building Inspectors and trainee inspectors must maintain and demonstrate professional competence.

Project information may therefore be used internally for legitimate purposes including:

- technical training;
- supervision;
- mentoring;
- competence assessment;
- RBI development;
- CPD;
- internal audit;
- peer review;
- quality assurance;
- performance evaluation; and
- preparation of evidence supporting professional competence.

Such use shall remain subject to this policy.

Where reasonably practicable, information not required for the training or assessment purpose should be redacted, pseudonymised or otherwise minimised.

Access to training material containing identifiable client or project information shall be restricted to authorised persons.

The use of a BCS project for an individual's training or competence assessment does not transfer ownership or control of the project information to that individual.

---

11. Competence Portfolios and Removal of Company Data

Employees and contractors must not remove complete project files, client databases, plans, correspondence archives or other BCS records for inclusion in personal competence portfolios.

Where an individual requires evidence of work undertaken while employed by BCS for a legitimate competence assessment or registration purpose, that evidence must be:

1. requested through the authorised BCS process;
2. reviewed by an authorised manager or supervisor;
3. limited to information reasonably necessary to demonstrate competence;

4. redacted or anonymised where appropriate;
5. checked for confidentiality, copyright, commercial sensitivity and data protection implications; and
6. expressly authorised for release.

BCS may provide a controlled extract, redacted evidence, supervisor's statement or other suitable evidence rather than permitting the employee to copy the underlying project file.

No employee or former employee is entitled to retain unrestricted copies of BCS project files merely because that individual worked on the project.

---

12. Ownership and Control of Information

Subject to third-party intellectual property and legal rights, records created or received by employees in the course of their employment and stored within BCS systems shall form part of the company's business and regulatory records.

Passwords, system access or possession of copies do not create ownership rights.

Upon termination of employment or engagement:

- system access shall be withdrawn;
- company equipment shall be returned;
- company documents shall be returned or securely deleted from authorised temporary locations;
- no BCS information shall be retained on personal devices or accounts; and
- continuing confidentiality obligations shall remain in force.

BCS shall nevertheless retain competence and development records where required to satisfy regulatory, legal or legitimate evidential obligations.

---

13. Secure Storage

BCS shall use appropriate technical and organisational measures to protect information.

Measures shall include, as appropriate:

- authenticated user access;
- password controls;
- multi-factor authentication;
- access permissions;
- controlled administrator privileges;

- firewalls and endpoint security;
- malware protection;
- software security updates;
- secure cloud and network storage;
- controlled backup arrangements;
- recovery arrangements;
- secure email systems;
- device encryption;
- access logging where available;
- secure disposal procedures; and
- periodic review of access permissions.

BCS shall take reasonable measures to ensure that its records remain available, identifiable, retrievable, protected and capable of electronic transfer throughout the required retention period.

---

14. Personal Devices and Removable Media

BCS project or personal information must not be permanently stored on privately owned devices.

Where mobile working is authorised, information must be accessed through BCS-approved applications or secure connections wherever reasonably practicable.

Use of removable media is prohibited unless specifically authorised.

Where temporary local storage is operationally necessary, information shall be transferred to the authorised BCS system and the temporary copy securely deleted as soon as reasonably practicable.

---

15. Passwords and User Accounts

Each user shall use their individually assigned account.

Users must not:

- disclose passwords;
- share accounts;
- allow another person to work under their credentials;
- leave authenticated systems unattended without appropriate locking; or

- attempt to access another user's account.

Access permissions shall be reviewed when employees change roles and withdrawn promptly when employment or contractual engagement ends.

---

16. Data Breaches and Security Incidents

Any actual or suspected:

- loss of information;
- unauthorised disclosure;
- incorrect email transmission;
- stolen device;
- compromised password;
- unauthorised system access;
- malware or ransomware incident;
- loss of paper records;
- unauthorised copying;
- unauthorised deletion; or
- other compromise of confidentiality, integrity or availability

must be reported immediately to the Managing Director, Quality Manager or person designated to manage data protection.

BCS shall assess the incident and determine whether notification to the Information Commissioner's Office, affected individuals, the Building Safety Regulator, insurer or another authority is required.

Data breaches shall be recorded and investigated as appropriate.

Corrective action shall be taken in accordance with the BCS Quality Management System.

---

17. Data Subject Rights

BCS shall maintain procedures for responding to individuals exercising applicable rights under UK data protection legislation, including rights relating to:

- access;
- rectification;
- erasure where applicable;
- restriction;

- objection; and
- other applicable statutory rights.

A request for deletion does not require BCS to destroy information where continued retention is lawful and necessary to comply with regulatory, statutory, contractual, insurance or legal obligations.

Requests shall be referred to the person responsible for data protection and shall not be dealt with informally by individual inspectors.

---

18. Accuracy and Document Control

Personnel shall take reasonable steps to ensure that records entered into BCS systems are accurate, identifiable and attributable.

Superseded drawings, reports or documents shall be identifiable where their retention forms part of the regulatory record.

No person shall alter, delete, overwrite or otherwise interfere with a regulatory record with the intention or effect of concealing:

- an earlier decision;
- correspondence;
- evidence;
- a contravention;
- an inspection finding;
- a professional judgement; or
- the history of the project.

Corrections should preserve an appropriate audit trail where this is necessary to demonstrate the regulatory history of the project.

---

19. ISO 9001:2015 Documented Information

BCS shall control documented information necessary for the effectiveness of its Quality Management System.

Controls shall address, where applicable:

- identification;
- description;
- format;

- review;
- approval;
- access;
- retrieval;
- distribution;
- storage;
- preservation;
- change control;
- retention; and
- disposition.

Externally generated documents necessary for BCS operations shall also be identified and controlled as appropriate.

---

20. Registered Building Inspectors

Every RBI working for or on behalf of BCS shall:

- comply with applicable data protection requirements;
- maintain confidentiality;
- use BCS technology responsibly;
- protect commercial and regulatory information;
- maintain appropriate competence in information security and data protection;
- comply with BCS information-management procedures;
- only access information required for authorised work; and
- report suspected information-security or data-protection failures.

An RBI's professional obligation to maintain evidence of competence does not override UK GDPR, confidentiality, intellectual-property, contractual or BCS information-security requirements.

---

21. Contractors and Third-Party Processors

Before providing third parties with access to protected information, BCS shall consider:

- the purpose of access;
- necessity;
- confidentiality;
- data protection responsibilities;

- information security;
- contractual controls;
- location of processing;
- retention and deletion arrangements; and
- whether a data-processing agreement or other contractual provisions are required.

Third-party access shall be limited to what is reasonably necessary.

---

22. Information Sharing with Regulatory Authorities

BCS may disclose information where lawfully required or authorised to do so to the Building Safety Regulator, local authorities, fire and rescue authorities, other statutory consultees, courts, law-enforcement bodies or other competent authorities.

Such disclosure shall be appropriately controlled and, where practicable, recorded.

Nothing in this policy shall prevent BCS from fulfilling a lawful statutory or regulatory obligation to provide information.

---

23. Disposal and Destruction

At the end of the applicable retention period, BCS shall determine whether information should:

- continue to be retained;
- be archived;
- be anonymised; or
- be securely destroyed.

Electronic records shall be securely deleted where appropriate.

Paper records containing protected information shall be shredded or disposed of through an authorised confidential-waste service.

Destruction shall be suspended where a legal, regulatory, insurance or investigation hold applies.

---

24. Staff Training and Awareness

All relevant personnel shall receive appropriate training concerning:

- UK GDPR;

- confidentiality;
- information security;
- cyber security;
- secure handling of building control records;
- phishing and fraudulent communications;
- data breaches;
- use of email;
- document control;
- retention requirements; and
- their responsibilities under this policy.

Training shall form part of induction and shall be refreshed periodically.

Training completion shall be recorded within the BCS Quality Management System.

---

25. Monitoring and Internal Audit

Compliance with this policy shall be monitored through the BCS ISO 9001 Quality Management System.

BCS may undertake:

- internal audits;
- access-permission reviews;
- file audits;
- training-record reviews;
- data-breach analysis;
- management reviews;
- corrective-action reviews; and
- sampling of project records.

Findings shall be recorded and corrective or improvement actions assigned where appropriate.

---

26. Breach of Policy

Unauthorised access, copying, downloading, disclosure, alteration, destruction or removal of BCS information may constitute:

- a breach of this policy;
- a breach of the employee's contract;

- misconduct or gross misconduct;
- a breach of confidentiality;
- a breach of data protection legislation;
- a breach of professional obligations; and/or
- an offence or civil wrong in appropriate circumstances.

BCS may investigate suspected breaches and take proportionate disciplinary, contractual, regulatory or legal action.

Where the conduct of a Registered Building Inspector may constitute a breach of applicable professional conduct requirements, BCS shall consider whether the matter requires referral to the relevant regulatory authority.

---

27. Regulatory and Jurisdictional Application

For work undertaken in England, BCS shall apply the requirements of the Building Safety Regulator, including the applicable Operational Standards Rules, Professional Conduct Rules for Registered Building Control Approvers and Code of Conduct for Registered Building Inspectors.

For work undertaken in Wales, BCS shall apply the corresponding Welsh legislative and regulatory requirements applicable to Registered Building Control Approvers and Registered Building Inspectors.

Where requirements differ between jurisdictions, the applicable statutory or regulatory requirement for the location of the building shall prevail.

---

28. Management Responsibility

The Directors of Building Control Surveyors Ltd have overall responsibility for ensuring that adequate arrangements exist for the protection and retention of information.

The Quality Manager or nominated Data Protection Lead shall be responsible for:

- maintaining this policy;
- coordinating data-protection compliance;
- maintaining appropriate retention arrangements;
- coordinating breach investigations;
- supporting staff training;
- monitoring compliance;
- ensuring corrective action where required; and
- reviewing regulatory changes.

Every person working for BCS remains individually responsible for information handled through their account or within the scope of their duties.

---

29. Management Review

The effectiveness of this policy shall be considered as part of BCS management review.

The review may consider:

- security incidents;
- data breaches;
- subject access requests;
- complaints involving information;
- regulatory changes;
- internal audit findings;
- access-control failures;
- training completion;
- information-retention performance;
- IT security arrangements;
- supplier performance; and
- opportunities for improvement.

---

30. Policy Review

This policy shall be reviewed at least annually and additionally following:

- significant changes to UK data protection law;
- changes to the Operational Standards Rules;
- changes to professional conduct requirements;
- significant IT-system changes;
- a material data breach;
- findings from internal or external audit;
- regulatory intervention; or
- significant organisational change.

The current controlled version shall be made available to relevant personnel.

SAMPLE STAFF DECLARATION

I confirm that I have read and understood the Building Control Surveyors Ltd Data Protection, Information Security, Confidentiality and Records Management Policy.

I understand that access to BCS databases, network storage systems and project information is provided solely for authorised employment, contractual, regulatory, training and competence purposes.

I understand that I must not retrieve, view, print, download, copy, transmit, disclose, retain or remove information except where authorised and necessary for the proper performance of my duties.

I understand that these obligations concerning confidentiality and company information may continue after my employment or engagement with Building Control Surveyors Ltd has ended.

Name: _____

Position / RBI Class: _____

Signature: _____

Date: _____

DOCUMENT CONTROL

Document: Data Protection, Information Security, Confidentiality and Records Management Policy
Reference: BCS-QMS-DP-01

Version: 1.0
Effective Date: _____
Review Date: _____
Approved By: _____
Document Owner: _____
Classification: Controlled – Internal / Public version as authorised
Retention: Superseded policy versions retained in accordance with BCS QMS document-control arrangements

END OF CONTROLLED DOCUMENT