ACS Construction Group

ACS OP 016 POLICY

ACS Privacy and Security Information Policy

POLICY TITLE	ACS Privacy and Security Information Policy		
ISSUE DATE	Sept 2024	**REVIEW DATE**	Sept 2025
VERSION	V1	**ISSUED BY**	HSEQ Systems Manager

ASSOCIATED DOCUMENTS	Data Protection Impact Analysis (DPIA); Change Management Process; New User Process; Leaving User Process; Business Continuity Plan;

APPROVED BY	Dave Curran (Commercial Director)	**DATE**	27/09/2024

REVIEW AND CONSULTATION PROCESS	This policy will be reviewed by the board of directors at least annually and by the Commercial Director as required. Changes and amendments will be review by the board and authorised for release at quarterly review meetings.
RESPONSIBILITY FOR IMPLEMENTATION AND TRAINING	The Commercial Director is responsible for the implementation of this policy and the training of staff in relation to the topics covered within the policy.

REVISION	DATE	AUTHOR	DESCRIPTION
Rev 1	27/09/24	HSEQ Systems Manager	Initial copy.

DISTRIBUTION	Document will be made available to all staff in Workspace.

Restricted © ACS Construction Group. All Rights Reserved.
Document is UNCONTROLLED when downloaded or printed.

Contents

1. Purpose and Scope 4

2. Responsibilities 4

3. Key Principles 4

4. Legislative Compliance 4

5. Information Security Controls 4

5.1 Employment Contracts 4

5.2 Training 4

5.3 Access Management 4

5.4 Passwords 5

5.5 Remote and Mobile Working 5

6. Asset Management 5

7. Data Classification 5

8. BYOD Policy 5

9. Software and Systems Management 5

10. Monitoring and Incident Response 5

11. Data Protection 6

12. Website Privacy Notice 6

12.1 Data Collection via Forms 6

12.2 Cookies 6

Restricted © ACS Construction Group. All Rights Reserved.
Document is UNCONTROLLED when downloaded or printed.

12.3 Data Storage and Retention 6

12.4 User Rights 6

13. Business Continuity 6

14. Policy Review 6

15. Further Information 6

Restricted © ACS Construction Group. All Rights Reserved.
Document is UNCONTROLLED when downloaded or printed.

1. Purpose and Scope

This Information Security Policy is a key component of ACS Construction Group business management framework and is designed to set out the requirements and responsibilities for maintaining the security of information within the business. The policy is supported by other policies and by guidance documents to assist in putting the policy into practice day-to-day.

2. Responsibilities

- **Managing Director**: Holds ultimate responsibility for information security.
- **Commercial Director**: Responsible for policy implementation, training, and oversight.
- **Line Managers**: Ensure team compliance.
- **All Staff**: Accountable for maintaining security standards.

3. Key Principles

- Compliance with relevant legislation and internal policies is mandatory.
- Systems access is restricted to authorised users based on business need.
- Security incidents must be reported to the Commercial Director.

4. Legislative Compliance

ACS Construction Group adheres to:

- Data Protection Act 2018 / GDPR
- Computer Misuse Act 1990
- Health and Safety Regulations
- Human Rights Act 1998
- Other applicable UK and international laws

5. Information Security Controls

5.1 Employment Contracts

- All contracts include confidentiality clauses.
- Identity verification is mandatory.

5.2 Training

- Annual training and ongoing awareness programs are mandatory for all staff.

5.3 Access Management

- Access is granted on a least-privilege basis.

Restricted © ACS Construction Group. All Rights Reserved.
Document is UNCONTROLLED when downloaded or printed.

- User and administrative access requires approval and is reviewed annually.
- Shared accounts are prohibited.

5.4 Passwords

- Minimum: 8 characters, including upper/lower case, numbers, symbols.
- MFA is mandatory where supported.
- Self-service reset and secure password creation are enforced.

5.5 Remote and Mobile Working

- Use of secure connections (e.g., tethered mobile internet) is required.
- Public Wi-Fi use is restricted without VPN.
- Devices must be encrypted and protected with strong PINs or biometrics.

6. Asset Management

- All assets must have designated custodians.
- Asset records are maintained accurately.
- Default settings and passwords must be changed before deployment.

7. Data Classification

Data is categorised as:

- **Unrestricted**: Public content.
- **Restricted**: Internal proprietary data.
- **Confidential**: Sensitive or personal data.

8. BYOD Policy

- BYOD is permitted only under strict compliance.
- Devices must meet patching, security, and monitoring requirements.
- ACS reserves the right to revoke BYOD access without notice.

9. Software and Systems Management

- All software must be licensed and approved.
- Critical updates applied within 7 days.
- Only authorised software may be installed via deployment tools.

10. Monitoring and Incident Response

- Staff have no expectation of privacy when using ACS systems.
- All incidents are logged, investigated, and reviewed by the Commercial Director.

Restricted © ACS Construction Group. All Rights Reserved.
Document is UNCONTROLLED when downloaded or printed.

11. Data Protection

- Data is backed up via OneDrive and third-party solutions.
- End-of-life data and devices are securely destroyed.

12. Website Privacy Notice

This section outlines how ACS Construction Group collects and processes personal information via its website:

12.1 Data Collection via Forms

- Data such as name, email, phone number, and message content is collected when users submit website forms.
- This information is used solely to respond to queries and provide requested services.

12.2 Cookies

- The website uses cookies to enhance user experience and gather analytics.
- Users may accept or reject cookies upon visiting the website.
- Cookies used include essential operational cookies and Google Analytics for anonymised visitor tracking.

12.3 Data Storage and Retention

- Personal data collected through the website is stored securely and retained only as long as necessary to fulfil the intended purpose.

12.4 User Rights

- Users have the right to request access to, correction of, or deletion of their personal data.
- Requests can be submitted through the contact information provided on the website.

13. Business Continuity

- Business Continuity Plans are reviewed and tested annually.
- Staff operate on cloud-based systems enabling remote continuity.

14. Policy Review

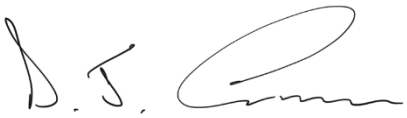
- Reviewed annually by the Commercial Director and the Board.
- Updates approved at quarterly review meetings.

15. Further Information

Restricted © ACS Construction Group. All Rights Reserved.
Document is UNCONTROLLED when downloaded or printed.

For guidance, contact the Commercial Director. Suggestions for policy improvements are welcome.

Policy Approved By



Dave Curran

27 Sept 2024

Restricted © ACS Construction Group. All Rights Reserved.
Document is UNCONTROLLED when downloaded or printed.