Cyber Security Policy

February 2026

Cyber Security Policy

1. Policy Brief & Purpose

This Cyber Security Policy outlines our guidelines and provisions for preserving the confidentiality, integrity, and availability of our data and technology infrastructure.

As a UK-based supplier of skilled, professional labour, we process and store:

- Employee personal data (1100+ workers)
- Applicant data
- Client contractual information
- Payroll and financial data
- Site access credentials
- Commercially sensitive tender information

We recognise increasing cyber risks, including ransomware, phishing, supply-chain compromise, and data breaches.

This policy is aligned with:

- UK General Data Protection Regulation
- Network and Information Systems Regulations 2018
- Good practice frameworks such as ICO/IEC 27001

We maintain a regulatory horizon-scanning process to monitor evolving UK cyber legislation and regulator guidance and are monitoring developments relating to the proposed UK Cyber Security and Resilience Bill. Upon enactment, a formal gap analysis will be conducted within 90 days and this policy will be updated accordingly.

2. Scope

This policy applies to all employees of Danny Sullivan Group Limited (DSG) and its subsidiaries (Danny Sullivan & Sons Ltd, Diamond Construction & Engineering Recruitment Limited, and Danny Sullivan Group Academy Limited), contractors, workers, agency workers, volunteers and any third party with access to our IT systems or data

3. Governance and Accountability

Cyber security is overseen at senior level.

- The Board retains ultimate accountability for cyber risk.
- A designated senior manager is responsible for operational cyber security.
- Cyber risks are reviewed at least annually by senior management.
- Significant cyber incidents will be escalated to the Board.

4. Confidential Data

Confidential data includes:

- Employee records and right-to-work documentation
- Payroll and bank details
- Client contract data
- Tender and pricing information
- Site access and security credentials
- Unpublished financial information
- Supplier agreements

All of us at DSG are required to protect this data and only access information necessary for their role.
We are the guardians of the personal data of colleagues and others and must respect and protect that data as if it was our own.

5. Device Security (Office & Site-based staff)

Given the mobile and distributed nature of construction operations:

All devices must:

- Be password protected (minimum 12 – character passphrases recommended)
- Use multi-factor authentication (MFA) where available
- Have disk encryption enabled
- Run centrally managed antivirus/anti-malware software
- Receive automatic security updates
- Be locked when attended
- Be remotely wipeable (company-issued devices)

Construction Site Considerations

- Devices used on-site must not be left unattended in vehicles.
- Shared site tablets must use individual logins.
- Public Wi-Fi must not be used to access company systems without approved VPN.

New hires receiving company equipment will receive setup instructions for:

- Disk encryption
- MFA enrolment
- Password management tool
- Endpoint security software

6. Email & Phishing Protection

Construction industry and related businesses such as DSG are frequent targets of invoice fraud and CEO impersonation scams.

Employees must:

- Treat urgent payment changes requests with caution
- Independently verify supplier bank detail changes by phone

- Avoid opening suspicious attachments
- Report phishing immediately to IT (email rezam@dannysullivan.co.uk)

Finance and payroll teams will receive enhanced phishing awareness training.

7. Password & Access Management

To protect our systems:

- Minimum 12-character passphrases required
- MFA mandatory for:
- Email
- Payroll systems
- Remote access (VPN)
- Cloud platforms
- Password sharing is prohibited unless formally authorized
- Privileged access is limited and reviewed quarterly
- Access is revoked immediately upon termination

A company-approved password manager must be used.

8. Data Transfer & Secure Handling

Employees must:

- Avoid transferring sensitive data outside company systems
- Use encrypted file-sharing tools approved by IT
- Never send payroll or personal data over unsecured email
- Verify recipients before sharing sensitive documents

Mass transfers of data must be approved by IT.

9. Incident Reporting & Response

All at DSG must immediately report:

- Suspected phishing
- Lost or stolen devices

- Unauthorised access
- Malware infections
- Data breaches

The IT function will:

- Log and classify incidents

- Contain and remediate threats
- Assess data breach reporting obligations under UK GDPR
- Notify regulators where legally required
- Escalate significant incidents to senior management

We maintain an Incident Response Plan and test it periodically.
We shall report notifiable cyber incidents within statutory timeframes where required by applicable legislation.

10. Supply Chain & Third- Party Security

As a labour supplier working with our clients on major construction and infrastructure projects, we rely on payroll providers, IT vendors, recruitment platforms, and subcontractors/suppliers/intermediaries.
We will:

- Conduct due diligence on key IT suppliers.
- Include data protection and cyber security clauses in contracts
- Limit third-party access to necessary systems only
- Review high-risk suppliers periodically

11. Business Continuity & Resilience

To ensure operational continuity:
- We maintain data backups (segregated and tested)
- Critical systems have recovery procedures
- Payroll continuity planning is in place
- Disaster recovery plans are documented
- Desktop cyber incident exercises are conducted periodically

Please refer to our IT Disaster recovery plan for more details.

12. Remote & Hybrid Working

Remote employees must:

- Use company-approved VPN
- Ensure home Wi-Fi is password protected
- Avoid use of shared family devices for company work
- Comply with all encryption and MFA requirements

13. Additional Security Measures

Employees must:

- Lock screens when away
- Report stolen equipment immediately
- Avoid suspicious downloads or websites
- Follow social media and internet usage policies
- Report potential vulnerabilities

IT/Security personnel must:

- Maintain firewalls and endpoint protection
- Monitor for unusual activity
- Deliver annual cyber awareness training
- Investigate breaches thoroughly
- Keep security controls under review

14. Training & Awareness

- All employees must complete annual cyber awareness training.
- High-risk roles (finance, payroll, HR, IT) will receive enhanced training.
- All new starters will complete cyber training within their first month.

15. Disciplinary Action

Failure to comply may result in disciplinary action in accordance with DSG policies.

Each case will be reviewed individually.

Russell Deards
General Counsel & Company Secretary
1st February 2026