Internal Policies for IT Usage and Conduct

February 2026

Internal Policies for IT Usage and Conduct

Purpose

Due to the continued growth of DSG and its increasing reliance on technology, this policy establishes the rules and controls required to ensure the secure, lawful, and responsible use of DSG's information systems, devices, networks, and data.

The purpose of this policy is to:

- Protect DSG against unauthorised access and security breaches
- Safeguard confidential and personal information
- Maintain the confidentiality, integrity and availability of DSG data
- Ensure compliance with applicable legal and regulatory requirements
- Promote responsible and professional use of company technology

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, visitors any third party with access to our IT systems or data.

All users are responsible for complying with this policy. Failure to comply may result in disciplinary action, up to and including termination of employment and contract.
The IT department is responsible for enforcing this policy and may update it as required.

Acceptable Use Policy (AUP)

The Acceptable Use Policy is a guideline on how to properly use the devices and networks with the organisation.

1) Prohibited Activities: Users must not take part in any illegal activities which includes fraud, data theft, hacking and any other activities that are illegal. Users must also refrain from using sites that are suspected to have malware or click on any untrusted links (anything that compromises the security of the network).

2) Respect for Intellectual Property: Users must be educated on any potential copyrights, the intellectual property rights of others and trademarks to avoid any infringements. (This policy is more directed towards the HR department).

3) Data Privacy: Users must protect all personal and sensitive data; users must not give unauthorised access to individuals at any given time. Users also must not share sensitive or personal information without the consent of the relevant person/department.

4) No Harassment: There will be no tolerance towards harassment, discrimination or abusive behaviour toward others.

5) Use of Resources: Users should avoid using the system resources excessively as it may negatively impact on the performance or experience of another user.

6) Monitoring and Enforcement: The IT department and the Leadership team have the right to monitor the usage of the employees at DSG to make sure that the policies are being carried out correctly; they also have the right to take any necessary actions against violations.

Security and Data Protection

The Security and Data Protection Policy is in place to help manage the data we have at DSG. These policies will ensure the confidentiality, integrity and availability of the data handled by DSG. The policy will go through the different types of data that are managed, whether it be digital or paper based.

1. **Data Reduction**: Users must only gather data that is essential for its intended purpose; it should only be collected for specific and genuine purposes. This helps to avoid collecting an excessive amount of data that is not required.

2. **Transparency:** Users must gather data in a way that is very clear for the relevant people to see so that any miscommunication can be avoided. Data must also be collected in compliance with the law.

3. **Accuracy**: Users must ensure that they keep all the data as accurate as possible. Users have a responsibility to rectify any inaccurate data that is found.

4. **Confidentiality:** Users must make sure that all the data is securely protected against any unauthorised access, loss or destruction.

5. **Passwords**: Passwords are put in place to deny access to unauthorised users. These passwords are initially provided to you by the IT department. If you are to change the password, ensure that you have the following: a minimum of 8 characters, at least 1 uppercase letter, at least 1 lower case letter, at least 1 number and at least 1 special character. Users must ensure that these passwords are not shared to others and are changed periodically.

6. **Access Control:** The IT department and Leadership team in DSG can authorise access to users, as well as the level of access the user has. Access over any required data will only be given to specific users.

7. **New Starters:** To ensure that a new starter joining DSG has all the correct access to platforms and the different equipment required, the line managers must complete the Typeform provided by the IT department by a minimum of 7 days before the start date of the employee.

8. **Encryption:** Sensitive and confidential data is encrypted to protect DSG from any data breaches, eavesdropping, tampering and more. Any data that is stored on hard drives or databases is encrypted which helps to prevent unauthorised access to the data if any of the physical media were to be stolen or lost. Any data that is transmitted through emails or other forms of communication is also encrypted (this is done through protocols like HTTPS or S/MIME).

Software and Hardware Management

The Software and Hardware Management Policy is put in place to give a guideline on how to manage all the provided software and hardware in DSG. This policy is also in place to help track the lifecycle of hardware and software used in the organisation.

1. **Software Inventory and License Management**: The IT department are responsible for keeping a list of all the different software used in DSG, as well as keeping track of the latest software versions, upgrades, updates, licenses and expiration dates. The IT department track the number of users for the software licenses and are required to be notified when the license is about to expire or has exceeded the limit for the number of users. In addition to this, only authorised users will have access to certain software.

2. **Regular Checks**: Software and Hardware are required to be checked and updated every few weeks if necessary. This is also to help ensure that there is compliance with legal requirements.

3. **Clean Desk:** Users must make sure that there is a good degree of cable management. Users must also shred any sensitive documents that are no longer needed; printer areas should also be clean to prevent any important documents falling into the wrong hands.

Incident Response

The Incident Response Policy is there to outline the required steps in the event of a security breach.

1. **Prevention:** The IT department is the identified Security Team of DSG: the purpose of this team is to reinforce the protocols. Employees across DSG must identify any sensitive data that requires protection. Employees are required to carry out monthly training to increase awareness on potential security threats and to get in the habit of reporting them. The IT department will also periodically test backup and recovery procedures to ensure that the data is secure in case of a breach. All the test results and training exercises will be noted in the Incident Response Plan document.

2. **Detection:** A potential security breach can be detected through DSG's antivirus software and firewalls. However, despite the use of varying software, users must still be alert to any suspicious activity and report it to the IT department immediately. All reported activity will be investigated and logged by the IT department.

3. **Containment:** As soon as the IT department confirm an incident, immediate action is required to be taken to reduce and prevent any further damage. The IT department will carry out a variety of things to ensure that the risk is contained, such as: deactivating any compromised accounts, isolating affected systems, blocking malicious network traffic and more.

4. **Eradication:** The IT department will investigate the cause of the incident and proceed with the necessary steps. Any malware and vulnerabilities will be removed.

5. **Recovery:** The IT department will look to restore the systems and data back to normality. This will be done through restoring backups and reinstalling/rebuilding affected software.

Compliance and Legal Requirements

The Compliance and Legal Requirements are there to ensure that the laws are being followed correctly. Through the different laws, users can maintain ethical standards in IT operations which helps protect sensitive information.

1. **Data Protection and Privacy**: Users must make sure that they comply with all the different local, national and international laws such as GDPR, CCPA, HIPAA. DSG strives to protect the privacy of all personal data.
2. **Intellectual Property Compliance**: All the different software, systems and data developed or bought by DSG belongs to the company. DSG prohibits any distribution,

copying and unauthorised use of software licenses; unlicensed software must not be installed on the systems as well.

3. **Patent and Copyright Compliance:** As stated before, users must make sure that no copyrighted or patented materials are in use to ensure prevention of copyright infringement.

4. **Compliance with Industry Standards**: DSG ensures compliance with industry standards such as ISO 27001 which makes sure that the different security risks for managing sensitive information is documented.

Remote Work and BYOD

Remote Work policy is in place to show the guidelines of what users can do when they work remotely or use a personal device (BYOD).

1. **Equipment:** DSG will provide users with any equipment (such as monitors, laptops, accessories) to improve comfortability of working remotely.

2. **Device Approval:** Users are required to request permission from the IT department for any personal devices that they want to use for work related purposes. The IT department will validate the security of the device that is requested.

3. **Reporting Lost or Stolen Devices:** Users must immediately report to the IT department if a personal device that was used for work purposes is stolen or lost; the IT department will take all the necessary steps to remotely wipe a device.

Potential Sanctions

After assessing and accepting these policies, any intentional breaches will result in a disciplinary action or even a termination of employment.
All employees, contractors and other users are required to adhere to these policies.

Final Note

All employees, contractors and third parties must confirm in writing that they have read, understood and agree to comply with this policy.

Russell Deards
General Counsel & Company Secretary
1st February 2026