CAREER SEEKERS DIRECT

Career Seekers Direct
Information Security Policy

1.0 Purpose

Information security is the framework of controls around policy, physical security, technical security, training, and organisational culture that help to protect the information that is valuable to Career Seekers Direct Ltd (CSD).

Information is essential for the day-to-day operation and functions of CSD -service delivery; knowledge exchange; administrative functions; partnership and community work.

CSD relies heavily on digital technology as well as on printed documents and records. Failure to adequately protect and secure information (whatever its form) could lead to serious data loss and compromise, cyber-incident, financial and reputational impact from which recovery could be difficult. CSD will implement information security controls and practices to safeguard its information, while also enabling staff, customers, visitors, and partners to access and use the information they need.

This Policy is based on the following standards, regulations, and legislation:

• UK General Data Protection Regulation (UK GDPR) and ICO Guidance
• Data Protection Act 2018
• Investigatory Powers (Interception by Businesses etc, for Monitoring & Record Keeping Purposes) Regulations 2018

2.0 Scope

Any individual who handles information on behalf of CSD as part of their work or role (staff, customers and third parties carrying out a CSD function) must adhere to this Policy. This policy relates to securing CSD information and working to ensure an appropriate balance of the confidentiality, integrity, availability and safety of the information and systems.

Sensitive information that is valuable to CSD (whether owned, generated by, or entrusted to CSD) should be protected from theft, misuse, or compromise that could impact:

• an individual's reasonable expectations of privacy, security, and safety.
• CSD's ability to carry out its work.
• CSD's reputation.
• CSD's ability to meet legal, ethical, and regulatory requirements.

Information can be written, electronic, or verbal and can include (but is not limited to):

- email correspondence;
- published documents;
- contact details;
- plans and strategy documents;
- data, analysis, and findings;
- information held on student and staff systems;
- disciplinary or grievance proceedings.

Whatever the form, valuable and sensitive information must be appropriately protected throughout its lifecycle (collecting, storing, using, sharing, retaining and disposal).

This policy supports and should be read in conjunction with (sits alongside) all the CSD GDPR policies.

3.0 Policy Statements:

Each staff member is responsible for assessing compliance with CSD Policy if in doubt we expect staff to request support about the appropriate level of safeguards. All staff must apply a combination of controls, to maintain and protect the confidentiality, integrity, availability, and safety of CSD information.

Four simple principles apply:
1. Know what you have
2. Assess the risks
3. Protect
4. Govern and Review

1. Know what you have - Requires clear ownership of and responsibility for assets.

A. Job Roles within CSD have specific information assets they relate to, and the role holder is the responsible Data Owner for that information. This will be recorded in the Records Management Schedule. Data Owners are responsible for ensuring their data is securely managed regardless of physical or online location in accordance with GDPR. What data is stored and what records management processing is applied to that data is to be stored in the Records Retention Schedule.
The Data Owner is responsible for putting rules and processes in place around access, use, quality and accuracy, storage and security, and ensuring compliance with those documented rules.

B. Asset Register
IT equipment, software and cloud services, and storage used by CSD is recorded within an Asset Register. Each hardware assets serial details are recorded in the asset register on arrival and deleted on secure disposal. CSD Admin, maintain an asset register of applications, systems, and services.

C. Training and Awareness
CSD is committed to supporting and promoting staff awareness of their information security responsibilities through a framework of policies, guidance, webpages, team briefings and staff obligatory e-learning. Training should be appropriate to role and data owned. For example, users with privileged access to systems who regularly handle personal information, should undertake bespoke training, and adhere to documented operating procedures. CSD Management organise and record the training of staff.

2. Assess the risks
When planning or developing new information systems and services, or new use of information, to be used within CSD, this should be done in conjunction with the CEO. This is to:
• ensure effective use of CSD resources (financial, infrastructure and workforce).
• prioritise workload against existing demands.
• ensure the system meets technical security baselines and enterprise architecture design principles

• assess the impact, and integration with current CSD systems.
• assess and build in data protection privacy and transparency requirements.

Data Classification: Assessing and classifying information using the Data classification Scheme focuses effort and resources into identifying and protecting the most sensitive and valuable information.

Data Classification
CSD uses the following three data classifications which underpin this Information Security Policy.

A Public Data

- Information intended for sharing in the public domain

Impact if breached:

- No adverse impact

Information classed as public does not need any special handling requirements.

B Internal Data

- Information used for day-to-day CSD functions not for general public
- Default classification

Impact if breached:

- Some adverse impact and disruption to services.
- Possible breach of confidence or statutory duty

Access should be:

- Appropriate to role and is protected by min. one barrier e.g., username and password for technical security.
- Internal Confidential ID access control or locked office / cupboard for physical security.
- Use approved IT (approved cloud and CSD premises)

C Confidential Data

- Any quantity of Personal data (about living people) or information with contractual, business or research value

Impact if breached:

- Serious privacy or reputational risk, financial impact, commercial disadvantage or disruption to services Breach of statutory / regulatory duty / risk of fine

Access should be:

- appropriate to role and protected;
- encrypted when in transit;
- shared only with appropriate personnel;
- securely destroyed at end of use

3. Protect

The best form of protection is to have a well-informed team. CSD requires staff to undergo assessed IT Security training which is reviewed annually. CSD staff are provided with advice on how to choose good passwords, these must be strong, unique and regularly updated. Passwords must be between 8 and 10 characters long with one numeric and one special character.

Paper records – are secured in locked cabinets at all times. IT hardware must not be left unattended in a school or a vehicle especially overnight, even if on the driveway.

Removable media such as USB Sticks are banned from use with CSD, with the only exception of use to deliver presentations when no personal data is present.

HQ provide and are responsible for ensuring IT facilities and services meet external security standards, self-assessments, audits, and other regulatory frameworks. CSD owned IT assets must conform to a standard which includes but is not limited to: Disk Encryption, Firewall enabled, currently Windows 11* minimum with Bitlocker, up-to-date Anti-Virus and Malware detection software set to run automatically and device lock after 2 minutes. Software on CSD IT assets is restricted to an approved software list. The standard is expanded upon below.

*The latest versions of operating systems, web browsers and applications must always be used.

Should it be necessary to transmit personal data with or without special characteristics to agencies external to CSD then arrangements would be made with that agency to ensure the data was adequately protected (possibly encrypted) during transit.

A. Minimum-security hardware baseline

Secure configuration of equipment including end user devices:

- Ensure that computers and devices are properly configured to reduce vulnerabilities and provide only the services required to fulfil their role.

Computer security

- Ensure that software (including operating systems and application systems) is licensed, supported, has automatic updates enabled

Anti-virus and anti-malware protection:

- Ensure real-time malware protection is installed on all devices.
- To restrict execution of known malware and untrusted software, from causing damage or accessing data

User access controls and management:

- A process to create and approve user accounts, remove or disable access in a timely manner when no longer required, implement a second layer to validate a user. A user access document is maintained.
- User Accounts must be protected with multi factor authentication, where this is available.

- Account and password management processes are in place

Encryption

- Helps protect sensitive data from unauthorised access

Backing up Regularly

- creating a copy of your information so you will always have a recent version of your information saved, which helps to recover quicker if your data is lost or stolen. Our Microsoft estate includes document backup and restore

Resilience and availability

- Information and services should be consistently and readily accessible for authorised parties and work as expected.
- All new and existing services should be assessed to ensure appropriate resilience and availability has been specified and built into the system and/ or support model.

CSD HQ will assess new systems and software to ensure that they meet the baseline security requirements to host, to access or to integrate with CSD data.

B. Information Handover and End of Use

All CSD information should be returned to CSD when users leave or move to another role (i.e., staff, students and third parties carrying out a CSD function). This includes informing appropriate staff of information handover arrangements to ensure CSD retains ownership and custody of the information. All members of CSD should comply with CSD's Records Management Schedule, Asset Register and User Management for end of use secure disposal or preservation of information.

Internal and Confidential information should be 'destroyed beyond the ability to recover it' (paying due regard to environmental and legislative requirements around waste and hazardous waste processing). Physical paper records are shredded at CSD HQ according to the Records Management Schedule Secure. End of life IT equipment is securely erased under a certified third-party Asset Disposal Partner.

C. Incident Reporting:

- All staff and CSD partners are jointly responsible for reporting data loss and security incidents.
- Report a loss or compromise of personal data immediately to CSD HQ.
- A core function of CSD HQ is to effectively investigate the cause(s) of an IT security incident and implement measures to recover and mitigate risk to CSD. It is important to learn from security incidents to continue to protect CSD, improve awareness and reduce recurrence. CSD HQ may pass information relating to an IT security incident or breach to external organisations for information or further action. These may include (but are not limited to) the Information Commissioner's Office (ICO), the Police or other Statutory bodies.

4. Govern and review

A security governance framework is not just policy compliance. It is about embedding responsibility for information across all aspects of CSD's work. Enabling the culture that

recognises the value and importance of data, how it underpins our business goals, and how it supports all aspects of CSD's research, teaching and learning, professional services, and wider collaboration. This Information Security Policy is part of the foundations supporting CSD to control, direct and communicate cyber security risk management activities.

Business Continuity

CSD's Business Continuity is overseen by the CEO, with contributions from all relevant areas of CSD. This includes maintaining, reviewing, and testing Business Continuity Plans (BCPs) to integrate with CSD's approach.

5. Policy Compliance

Failure to comply with this Policy and the Information Protection Guide in protecting CSD's information (or that entrusted to us by a third party) puts CSD at risk of reputational damage, financial penalty, breach of legal, contractual or regulatory requirement. It may also lead to disciplinary action in accordance with the relevant Disciplinary Policy.

6. Related Documentation

This section lists directly relevant guidance and policies that have been referenced within this Information Security Policy. This policy is subject to bi-annual review which includes a check that hyperlinks within the document are active and up to date.

Policies and standards

- A2 Data Management Policy
- C1 Data Protection Policy
- D1 Data Subject Rights
- E1 Privacy Notices
- Asset Register
- Risk Register
- User Management records
- Data Protection Impact Assessment register
- Data Breach register
- Retention Management Schedule
- Disaster Recovery Plan

Policy Review

Review due: Biannually by January 2026