



Section	Client
Policy Title	Privacy

1. LEGISLATION

Privacy Act 1988 – Commonwealth
Information Privacy Act 2000
Privacy and Data Protection Act 2014
National Disability Insurance Scheme 2013 - Commonwealth

2. STANDARD/S

Department of Human Services Standards (DHS) (2014)
National Standards for Disability Services (DSS) (2012)
NDIS Practice Standards 2018
Australian Privacy Principals

3. PURPOSE

This policy provides ConnectGV with a framework for maintaining privacy and confidentiality of data.

Every Staff member at ConnectGV entrusted with keeping information confidential has an obligation to keep relevant Information safe from theft or unauthorized access.

All Staff and those acting on behalf of ConnectGV who have access to confidential information are to ensure that information is treated in accordance with this policy.

In addition delegates are responsible for immediately reporting any suspected violation(s) of this policy.

Breaching this policy may lead to dismissal and / or legal action.

4. POLICY STATEMENT

All ConnectGV staff with authorised access to confidential information stored on ConnectGV systems or in any media format are required to protect this information. All staff and those acting on behalf of ConnectGV:

- a) will access confidential information for the sole purpose of performing their job-related duties;
- b) will not seek personal benefit or permit others to benefit personally from any confidential information that comes to them through their work assignments;
- c) will not permit unauthorised use of any confidential information that can be found on ConnectGV systems or in any media format;
- d) will not enter, add, change, or delete confidential information if not authorised to do so;
- e) will not release or disclose confidential information other than what is required to perform their job-related duties and in accordance with applicable ConnectGV policies and procedures on releasing or disclosing confidential information;
- f) will not exhibit the contents of any confidential information to any person unless it is necessary to perform their job-related duties and in accordance with all applicable ConnectGV policies and procedures on exhibiting confidential information;
- g) will keep personal passwords confidential and will not disclose them to anyone within or outside the organisation. Forgotten passwords and suspected compromises of passwords should be reported immediately;
- h) will strive to keep confidential information on systems from being viewed by others (other than to whom the information is related to e.g. the client or their family member,



Section	Client
Policy Title	Privacy

primary carer) and will strive to ensure that computer screens are locked when away from their desk or office;

- i) will strive, for training purposes, to use simulated training information when possible; when this is not possible, will strive to protect and/or disguise any confidential information used; and
- j) will strive to dispose of confidential information in accordance with applicable laws and ConnectGV policies on record retention.
- k) will not discard any confidential information in a waste receptacle or recycling bin (if applicable); will shred hard copy confidential information prior to disposal or dispose via confidential waste disposal means.
- l) will not remove confidential information from work premises without permission.

5. RESPONSIBILITY FOR IMPLEMENTATION, COMPLIANCE MONITORING, MEASURING AND CONTINUAL IMPROVEMENT

These management positions are responsible for implementation and compliance monitoring of the policy in their work areas:

- Chief Executive Officer (CEO)- Risk Management
- General Manager Finance- Information Technology Risk Management
- Company Secretary- Freedom of Information Requests and Approval process
- Manager Future Directions- Client Confidentiality
- General Manager, People Performance & Culture- Employee Confidentiality

6. SCOPE OF POLICY

This Policy applies to all client confidential information held by ConnectGV. Staff members at ConnectGV who monitor and enforce compliance with this policy are responsible for ensuring that they remain compliant with relevant legislation at all times.

7. DEFINITIONS

Applications – Means all software that connects to, or is accessed via, the ConnectGV network. Applications include but are not limited to internet, intranet, email, client management systems, HR/Payroll systems, Incident Management systems, and financial systems and Policies Procedures systems.

Confidential Information – means:

- a) information held by ConnectGV that may harm the person to whom it refers/belongs if seen or acquired by a person not authorised by ConnectGV policy, procedure or applicable external regulations;
- b) information that is protected by federal or state legislation dealing with privacy; and examples include:
 - i. name, birth date, race, gender, marital status, disability status, citizenship;
 - ii. home address, home telephone number(s), relatives names, addresses, and telephone numbers;
 - iii. employee files;
 - iv. an employee's employment status, including leave of absence information, appointment begin and end dates, termination date, termination reason;



Section	Client
Policy Title	Privacy

- v. an employee's payroll information, including salary rates, tax information, withholdings, direct deposit information;
- vi. ConnectGV finance information, including rates and investments;
- vii. ConnectGV operating plans, including strategic, business, and marketing plans;
- viii. ConnectGV facilities management documentation, including security system information;
- ix. ConnectGV auditing information, including internal audit reports and investigative records; and
- x. ConnectGV organisational legal documents, including pending lawsuits and attorney-client communications.

Information – Means all data, system records, information, reports, images and videos that may be held, transmitted, stored or received in ConnectGV systems, applications, or in hard copy format.

Systems – Means all equipment and devices that connect to the ConnectGV network. Equipment and devices includes, but is not limited to, desktop computers, laptops, smartphones, tablets, printers, data and voice networks, networked devices, software, electronically-stored data, portable data storage devices, third party networking services, telephone handsets, video conferencing systems, and all other similar items commonly understood to be covered by this term.

Staff – Is every employee who has access to any of ConnectGV systems, applications and networks. This includes permanent employees and also temporary employees, contractors, agencies, consultants, suppliers, clients and business partners.

8. RELATED DOCUMENTS/LINKS

- Risk Management Policy
- Consent Policy
- Code of Conduct Policy
- Conflict of Interest Policy
- Open Disclosure Policy

Accountable	CEO
Responsible	General Managers
Review Date	22 Nov 2022

REVISION HISTORY

Revision Ref. No.	Approved/ Amended/ Rescinded	Approval Date	Management	Committee/ Board	Document Reference
V1	Approved	27/04/2016	CEO	Board	Client
V2	Amended	22 Nov 2019	Management	CPAR	Client