ABN 18 085 501 837

DATA PROTECTION POLICY

PURPOSE

CG Spectrum Institute (**CGSI**) Processes Personal Data in the ordinary course of its business operations, including Personal Data relating to:

- its students (potential, current and alumni);
- its employees and contractors;
- users of its website; and
- other stakeholders.

In Processing Personal Data, CGSI is subject to:

- the *Privacy Act* 1988 (Cth) including the *Australian Privacy Principals* (**APP**);
- the Spam Act 2003 (Cth);
- relevant State legislation;
- the European Union (**EU**) General Data Protection Regulation 2016/679 (**GDPR**) to the extent it offers courses (free or paid) or monitors the behaviour of individuals (such as website analytics) of individuals in the EU;
- the UK GDPR (which has the meaning given to it in section 3(10) (as supplemented by section 205(4)) of the *Data Protection Act* 2018 (UK), to the extent it offers courses (free or paid) or monitors the behaviour of individuals (such as website analytics) of individuals in the UK; and
- any other law, regulations, standards, guidelines, and directives relating to privacy and data protection for which CGSI is bound.

These laws dictate how CGSI may lawfully carry out its activities and the safeguards implemented to protect Personal Data.

The purpose of this Data Protection Policy is to set out key legislative provisions and to describe the steps CGSI must take to ensure that it complies with the same.

IMPLEMENTATION OF POLICY

This policy applies to all Personal Data that CGSI Processes.

All officers, employees, contractors and other third parties that have access to CGSI systems are responsible for implementing this policy. However, the following departments have key areas of responsibility:

The **Board of Directors** has the overall responsibility of ensuring that CGSI complies with its legal obligations.

The **General Counsel** or **Data Protection Officer** is responsible for:

- reviewing CGSI's data protection policies and procedures to ensure conformity with applicable laws;
- ensuring adherence to CGSI's policies and procedures;
- reviewing all data processing agreements and related contracts with third parties;
- arranging data protection training and providing relevant advice or guidance for persons covered by this policy;
- addressing any queries, complaints, or access requests from Data Subjects; and
- ensuring the board of directors of CGSI is updated on key data protection matters and risks.

The **IT Team** (whether internal or outsourced and monitored by the CEO) is responsible for:

- ensuring appropriate technical measures are implemented in Processing Personal Data;
- regularly evaluating technical measures employed by CGSI and third-party services used by CGSI; and
- ensuring all systems, services, and hardware meet acceptable security standards and are regularly checked or scanned to safeguard those systems, services, and hardware.

The **Marketing Team** are responsible for ensuring that all marketing initiatives abide by data protection principles and where required, seek assistance from other appropriate departments to confirm the same.

All **Students** are responsible for acting within the scope of this Data Protection policy and reporting any actual or suspect Personal Information breach.

DEFINITIONS

In this Data Protection Policy:

TERM	MEANING
Consent	of the Data Subject, means any freely given, specific, informed, and unambiguous indication of the Data Subject's wishes by which he or she, by a statement or by a clear affirmation action, signifies agreement to the processing of Personal Data relating to him or her.*
Controller	means the natural or legal person, public authority, agency, or other body which, alone or jointly with others, determines the purposes and means of the Processing of Personal Data.*
Personal Information or Personal Data	In Australia, **"personal information"** means information or an opinion about an identified individual, or an individual who is reasonably identifiable: (a) whether the information or opinion is true or not; and (b) whether the information or opinion is recorded in material form or not. Under the GDPR, **"personal data"** means any information relating to an identified or identifiable natural person (**Data Subject**); an identifiable

	natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person.*
Processing	any operation or set of operations which is performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaption or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.*
Sensitive Information or Special Category Personal Data	In "Australia", "**sensitive information"** means: (a) information or an opinion about an individual's: (i) racial or ethnic origin; (ii) political opinions; (iii) membership of a political association; (iv) religious beliefs or affiliations; (v) philosophical beliefs; (vi) membership of a professional or trade association; (vii) membership of a trade union; (viii) sexual orientation or practices; or (ix) criminal record; (b) health information about an individual; (c) genetic information about an individual that is not otherwise health information; (d) biometric information that is to be used for the purposes of automated biometric verification or biometric identification; or (e) biometric templates. Under the GDPR, **"special category personal data"** means Personal Data that reveals racial or ethnic origin, political beliefs, religious or philosophical beliefs, trade union membership, genetic data, biometric data for purposes of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation. *

***Note:** Definitions extracted from the GDPR.

DATA PROTECTION PRINCIPLES

Australia

1. CGSI is committed to Processing Personal Information in accordance with its obligations under the **APPs** (and other laws set out in section 1). The APPs require CGSI to:

   (a) (**Compliance, Management and Transparency**): implement open and transparent privacy practices, procedures and systems that:

- ensure compliance with the APPs;
- enable CGSI to deal with inquiries and complaints from Data Subjects.

(b) (**Privacy Policy**): develop and make readily available a policy about its management of Personal Information.

(c) (**Anonymity and pseudonymity):** entitle Data Subject to have the option of anonymity or using a pseudonym, except where impracticable or another prescribed exception applies.

(d) (**Collection of Personal Information**):

- collect Personal Information only where reasonably necessary for one or more of its legitimate functions or activities;
- require Personal Information to be collected directly from the Data Subject to whom it relates, unless impracticable or another prescribed exception applies; and
- obtain the Consent from the Data subject in order to collect Sensitive Information, or another prescribed exception applies.

(e) (**Unsolicited Personal Information**): determine whether it has grounds to collect any unsolicited personal information (in accordance with clause 4.1.1(d) and APPs 3) and:

- where it does have such grounds, to ensure compliance with the remaining APPs; or
- where it does not have such grounds, to destroy or de-identify the Personal Information (provided it is lawful and reasonable to do so).

(f) (**Notification):** notify a Data Subject (or ensure they are aware), at or before the time of collection, of prescribed APPs matters, including but not limited to:

- whether the Data Subject's Personal Information is collected from third parties;
- the purpose of the collection;
- to whom Personal Information is disclosed;
- the processes through which a Data Subject can access and/or correct their Personal Information; and
- the processes through which a Data Subject can complain about the way in which their Personal Information is handled.

(g) (**Use or Disclosure**):

- not use or disclose Personal Information for a purpose other than for the purpose it was collected, unless the Data Subject consents; or
- the Data Subject would reasonably expect their Personal Information be used for the secondary purpose; or
- another prescribed exception applies.

(h) (**Direct Marketing**): not allow Personal Information to be used for direct marketing purposes, unless the Data Subject reasonably expects it, or consents to it and prescribed 'opt out' processes are in place through which the individual can elect not to receive direct marketing communications (and the individual has made this election).

(i) (**Cross Border Transmission and Disclosure**): take reasonable steps (such as impose contractual obligations) to ensure any international recipient of Personal Information from CGSI does not breach the APPs. CGSI is not required to comply with this obligation if the international recipient is bound by laws that protect Personal Information in a substantially similar way or above that of the APPs, or the Data Subject consents to the disclosure in the knowledge that their consent will negate this obligation.

(j) (**Government Related Identifiers**): not adopt, use or disclose a Government-related identifier (e.g. tax file number, passport number or medicare number) unless:

- required or authorised by law;
- necessary to verify a Data Subject's identity; and/or
- another prescribed exception applies.

(k) (**Quality**): take reasonable steps to ensure the Personal Information it Processes is accurate, up to date and complete.

(l) (**Purpose**): ensure Personal Information is only Processed to the extent to which it is relevant to the purpose of the Processing.

(m) (**Security**):

- take reasonable steps to protect information from misuse, interference and loss and from unauthorised access, modification, or disclosure.
- destroy or de-identify Personal Information that is no longer requires (unless otherwise required to be retained by law).

(n) (**Correction**): take reasonable steps to correct personal information:

- upon request from a Data Subject; or
- where it reasonable believes, having regard to the purpose to which CGSI holds the Personal Information, that the Personal Information is inaccurate, out-of-date, incomplete, irrelevant or misleading; and
- If CGSI refuses a request for correction, it must provide reasons to the Data Subject; or
- If CGSI does correct the information, it must notify third parties to which the Personal Information was disclosed.

2. Information in relation to CGSI's privacy practices, procedures and systems in compliance with the APPs is set out in CGSI's Privacy Policy.

European Union and United Kingdom

1 CGSI is committed to Processing Personal Information in accordance with its obligations under the GDPR and UK GDPR to the extent it applies to UK or EU Data Subjects. Under Article 5 of the GDPR, Personal Data shall be:

(a) (**Lawfulness, fairness, and transparency**): processed lawfully, fairly and in a transparent manner.

(b) (**Purpose limitation**): collected for specific, explicit, and legitimate purposes and must not be further processed in a manner incompatible with those purposes.

Where personal data is processed for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) of the GDPR, it will not be considered incompatible with the initial purposes.

(c) (**Data minimisation**): adequate, relevant, and limited to what is necessary.

(d) (**Accuracy**): accurate and, if required, kept up to date.

If data is inaccurate, reasonable steps must be taken (with regard to the purpose for which it is being processed), that the data is rectified or erased without delay.

(e) (**Storage limitation**): kept in identifiable form for no longer than necessary for the purposes in which it is processed.

Personal data may be stored for longer periods where it is processed for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) of the GDPR and subject to appropriate technical and organizational measures.

(f) (**Integrity and confidentiality**): processed with appropriate technical and organisational measures, including protection against unauthorized or unlawful processing, accidental loss, destruction, or damage.

2 Under Article 6 of the GDPR, Personal Data can be lawfully processed where at least one of the following applies:

(a) (**Consent**): where the Data Subject provides Consent for one or more specific purposes;

(b) (**Contractual Performance**): where Processing is necessary for the purpose of a contract, which the Data Subject is a party or in order to take steps prior to entering into a contract;

(c) (**Legal Requirement**): where processing is for compliance with a legal obligation to which the Controller is subject;

(d) (**Vital Interest**): where processing is to protect the vital interests of the Data Subject or another person;

(e) (**Public Interest**): where processing is for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller; or

(f) (**Legitimate Purpose**): where processing is for the legitimate interests pursued by the Controller or by a third party, except where this is overridden by the interests, rights and freedoms of the Data Subject which require protection of Personal Data, such as children.

3. To confirm Personal Data can be lawfully processed for EU and UK Data Subjects, CGSI must:

(a) ensure that the lawful basis for Processing Personal Data is recorded in the Register of Processing Activities;

(b) ensure it will retain well-reasoned documented evidence where the lawful basis for Processing Personal Data is required to protect the vital interests of the Data Subject or of another natural person; or if required to perform a task that is believed to be in the public interest or part of an official duty; or it is in the legitimate interests of CGSI and is judged not to affect the rights and freedoms of the Data Subject in a significant way;

(c) (**Consent**) where the lawful basis for Processing Personal Data is based on Consent:

(i) record and retain evidence of Consent of the Data Subject;

(ii) if the Data Subject is under the age of 16 years (a lower age may be allowable in specific EU member states), parental consent must be obtained. The USA Federal Children's Online Privacy Protection Act requires verifiable parent Consent prior to the collection of any Personal Data from children under 13 years old;

(iii) if the Consent is obtained by a third-party on behalf of CGSI, the third-party must be under a contractual obligation to:

A. obtain the Consent from the Data Subject (or parent or guardian, as applicable); and

B. provide evidence of the Consent to CGSI.

(iv) the Data Subject must be provided with clear and transparent information in writing about their rights (as set out in section 8) and usage of their Personal Data at the time Consent is obtained; and

(v) if Personal Data is not obtained directly from the Data Subject, then the information set out in (c) (iv) above, must be provided to the Data Subject within a reasonable period (not more than one (1) month) after the Personal Data is obtained.

(d) (**Contractual Performance**) where the lawful basis for Processing Personal Data is required to fulfil a contract with the Data Subject, Consent is not required. This will generally apply where the terms of the contract cannot be fulfilled with the Personal Data; and

(e) (**Legal Requirement**): where the lawful basis for Processing Personal Data is required to comply with an applicable law, Consent is not required. For example, this may apply to some Personal Data related to employment and taxation.

COMPLIANCE

1. To ensure compliance with the Data Protection principles in Australia, EU and UK, CGSI must:

- maintain relevant data protection and IT policies, which are readily accessible;
- provide appropriate data protection training of its officers, employees, and contractors;
- maintain and regularly review its technical and organisational measures; and
- properly document its practices, procedures and systems.

SENSITIVE INFORMATION OR SPECIAL CATEGORY PERSONAL DATA

As part of its business, CGSI may Process Sensitive Information or Process Special Category Personal Data. Both in Australia and under the GDPR, a greater level of protection is afforded to Sensitive Information or Process Special Category Personal Data.

Australia

Unless an exception applies, in Australia:

- the Data Subject must consent to the Processing of Sensitive Information; and
- the Processing of Sensitive Information must be reasonably necessary for CGSI's legitimate functions or activities.

European Union and United Kingdom

For EU and UK Data Subjects, Processing Special Category Personal Data is prohibited, **unless** one of the ten (10) conditions under Article 9 of the GDPR applies. CGSI must:

(a) ensure that one of the exceptions set out in Article 9 of the GDPR is met and recorded in the Register of Processing Activities; and

(b) if it relies on Consent, ensure explicit Consent is obtained in accordance with section 4.2.3(c).

ABN 18 085 501 837

RIGHTS OF THE DATA SUBJECT

Australia

1. In Australia, Data Subject have the following rights (unless an exception applies);

- the right to be informed;
- the right of rectification;
- the option to not identify themselves, or use a pseudonym;
- the right of access;
- the right to make an enquiry or compliant; and
- the right to stop receiving unwanted direct marketing.

2 All Data Subjects must be notified of these rights.

European Union and United Kingdom

1. For EU and UK Data Subjects, CGSI must comply with Articles 12 to 23 of the GDPR. Data Subjects covered by the GDPR are entitled to the following:

- the right to be informed;
- the right of access;
- the right of rectification;
- the right of erasure;
- the right to restrict processing;
- the right to data portability;
- the right to object; and
- rights in relation to automated decision making and profiling.

2. Under the GDPR, the following times periods apply to the rights of Data Subjects:

Data Subject Right	Time Period
The right to be informed	If Personal Data is supplied by the Data Subject, at the time Personal Data is collect. If Personal Data is not supplied by the Data Subject, within one (1) month of the time the Personal Data is obtained.
The right of access	Within one (1) month.
The right to rectification	Within one (1) month.
The right to erasure	Without undue delay
The right to restrict processing	Without undue delay
The right to data portability	Within one (1) month.
The right to object	On receipt of objection

Rights in relation to automated decision making and profiling	Not specified.

3. All EU and UK Data Subjects must be notified of these rights.

4 All EU and UK Data Subject requests must be handled in accordance with the Data Subject Request Procedure and recorded on the Data Subject Request Register.

PRIVACY BY DESIGN AND DEFAULT

1. (**Design**): CGSI has adopted the principle of privacy by design and must ensure that the definition and planning of all new or significantly changed systems that Process Personal Data will be subject to due considerations to ensure that appropriate technical and organisational measures are implemented, including the completion of one or more Data Protection Impact Assessments. The Data Protection Impact Assessments shall include:

   (a) consideration of how Personal Data will be Process;

   (b) consideration of the purpose for Processing the Personal Data;

   (c) an assessment of whether the proposed Processing of Personal Data is both necessary and proportionate to the purpose(s);

   (d) an assessment of the risks to Data Subjects in Processing the Personal Data; and

   (e) what controls are necessary to address the identified risks and demonstrate compliance with applicable laws.

2. (**Security**): CGSI shall implement appropriate technical and organisational measures to ensure a level of security appropriate to risk (in particular, accidental, or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored, or otherwise processed), including:

   (a) the pseudonymization and encryption of Personal Data;

   (b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;

   (c) the ability to restore the availability and access to Personal Data in a timely manner in the event of a physical or technical incident; and

   (d) a process of regular testing, accessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the Processing.

3. CGSI must take measures to ensure that only Personal Data which is necessary for each specific purpose of Processing is Processed.

CONTRACTS INVOLVING THE PROCESSING OF PERSONAL DATA

CGSI will ensure that all relationships:

(a) which are with a Data Controller or Data Processor with an establishment in the EU or UK; or where Processing activities relate to the offering of goods or services to persons in the EU or UK; or monitor the behaviour of persons in the EU or the UK, are subject to a documented contract that includes the specific information and terms required by the GDPR; or

(b) which are with any jurisdiction, other than those referred to in section 8(a) above, in which Personal Data is Processed, are subject to a documented contract that includes the specific information and terms required by the laws which govern that contract and the Personal Data that is Processed and the third party must comply with the APPs unless their local laws provide for a similar level of data protection or greater.

INTERNATIONAL TRANSFERS OF PERSONAL DATA

Australia

CGSI may only transfer Personal Information outside of Australia if it has taken appropriate steps to ensure that the third party:

(a) will comply with the APPs in respect of the transferred Personal Information while it remains in its possession or under its control; and

(b) the recipient outside of Australia is bound by legally enforceable obligations to provide a standard or protection to the Personal Data transferred that is comparable to that under the APPs; or

(c) the Data Subject unequivocally consents.

European Union and United Kingdom

Transfers of Personal Data outside the European Union or United Kingdom will be carefully reviewed prior to the transfer taking place to ensure that they fall within the limits imposed by the GDPR. This may depend as to the adequacy of safeguards for Personal Data applicable to the recipient, which may change from time to time. Where an adequacy decision does not exist for the recipient in the destination country, an appropriate safeguard such as standard contractual clauses will be used, or a relevant exception identified as permitted under the GDPR.

BREACH NOTIFICATION

It is CGSI policy to be fair and proportionate when considering the actions to be taken to inform affected parties regarding breaches of Personal Data.

All breaches must be managed in accordance with the Information Security Incident Response Procedure and Personal Information Breach Notification Procedure.

AUTHORITIES

The following are the responsible authorities:

Jurisdiction	Responsible Authority
Australia	Office of the Australian Information Commissioner 175 Pitt Street Sydney New South Wales, Australia 2000 www.oaic.gov.au
European Union	Details of each applicable member state.
United Kingdom	Information Commissioner's Office Wycliffe House Water Lane, Wilmslow Cheshire SK9 5AF www.ico.org.uk

COMPLIANCE

1. (**Compliance Measurement**): The IT team and legal department must verify compliance with this Data Protection Policy and can do so through various methods, including (but not limited to), business tool reports, internal and external audits and feedback to the policy owner.

2. (**Continual Improvement**): This policy must be reviewed and updated as part of the continual improvement process.

3. (**Non-Compliance**): Any team member found in violation of this Data Protection Policy may be subject to disciplinary action, up to and including termination of employment or services.

RELATED

- Data Protection Policy;
- Privacy Policy;
- Significant Incident and Data Breach Policy;
- Personal Information Breach Notification Procedure;
- Data Protection Impact Assessment Procedure (EU & UK);
- Records of Processing Activities (EU & UK);
- Data Subject Request Register;
- Records of Processing Activities;
- Personal Data Breach Register; and
- Data Protection Impact Assessment Tool

ABN 18 085 501 837

VERSION CONTROL

VERSION	DATE	REVISION AUTHOR	APPROVED BY	SUMMARY OF CHANGES	NEXT REVIEW
V1.0	27 March 2023	LMP	Board of Directors	Establishment of policy	2025