THE ENGINEERING LINK GROUP (TELG)

PRIVACY & INFORMATION GOVERNANCE FRAMEWORK MANUAL

Version: 1.0

Document Owner: Greg Millican

Approved By: TELG Board

Review Cycle: Biennial (Every 2 Years)

Next Review Date: June 2028

1. PURPOSE

The Engineering Link Group (TELG) is committed to protecting the privacy, confidentiality, integrity and security of personal information collected through its programs and operations.

TELG operates educational STEM programs and events involving secondary school students, teachers, universities, industry partners and sponsors. The organisation recognises that participants and stakeholders entrust TELG with personal information and expects that information to be managed responsibly.

This Framework establishes the governance structure, principles, responsibilities and procedures that guide the collection, use, storage, disclosure, retention and destruction of information held by TELG.

The Framework provides a foundation for compliance with relevant privacy, child protection and information security obligations and supports TELG's commitment to ethical information management.

2. SCOPE

This Framework applies to:

- TELG Board members
- Employees
- Contractors
- Event personnel
- Third-party service providers acting on behalf of TELG

This Framework applies to information collected through:

- Engineering Link Project (ELP)
- Engineering Link Roadshow
- Bridge Competitions (Queensland and New South Wales)
- STEM-Sell

- Teacher professional learning programs
- University partnership activities
- Sponsor-supported activities
- Website enquiries
- Event registrations
- Marketing and communication activities

## 3. LEGISLATIVE AND REGULATORY FRAMEWORK

TELG will align its privacy practices with the following legislation and recognised standards:

Commonwealth

- Privacy Act 1988
- Australian Privacy Principles
- Spam Act 2003
- Corporations Act 2001 (where applicable)

Queensland

- Information Privacy Act 2009
- Child Protection Act 1999
- Working with Children (Risk Management and Screening) Act 2000

Other References

- Australian Cyber Security Centre Essential Eight
- Child Safe Standards
- Good Governance Principles for Not-for-Profit Organisations

## 4. INFORMATION GOVERNANCE PRINCIPLES

TELG adopts the following principles:

Principle 1 – Lawful Collection

Information will only be collected where reasonably necessary for TELG functions.

Principle 2 – Data Minimisation

Only the minimum information required will be collected.

Principle 3 – Purpose Limitation

Information will only be used for the purpose for which it was collected unless authorised or required by law.

Principle 4 – Security

Information will be protected against unauthorised access, disclosure, modification and loss.

Principle 5 – Transparency

Individuals will be informed about why information is collected and how it will be used.

Principle 6 – Accountability

TELG will monitor compliance and respond appropriately to privacy concerns and incidents.

5. INFORMATION HELD BY TELG

TELG may collect:

Participant Information

- Student name
- School
- Year level
- Parent/carer contact details
- Emergency contact details

Sensitive Information

- Medical conditions relevant to participation
- Allergies
- Dietary requirements
- Accessibility requirements

Event Information

- Program selections
- Attendance records
- Competition participation records

Media Information

- Photographs
- Video recordings
- Media consent preferences

TELG does not routinely collect:

- Medicare card information
- Family doctor details
- Full residential addresses

## 6. GOVERNANCE STRUCTURE

### Board Responsibilities

The Board is responsible for:

- Approving governance policies
- Monitoring compliance
- Reviewing significant privacy incidents
- Reviewing governance performance

### Policy Owner Responsibilities

The Policy Owner is responsible for:

- Maintaining this Framework
- Coordinating policy reviews
- Managing privacy incidents
- Monitoring implementation

The Policy Owner is:

Greg Millican

### Operational Responsibilities

Personnel handling information must:

- Follow TELG policies
- Maintain confidentiality
- Report privacy concerns immediately

## 7. INFORMATION LIFECYCLE MANAGEMENT

### Collection

Information must only be collected through approved processes.

### Use

Information must only be used for approved purposes.

### Storage

Information will be stored using approved systems including:

- Microsoft 365
- SharePoint
- Event Espresso

Access

Access will be restricted according to operational requirements.

Retention

Information will be retained according to the Records Retention and Disposal Schedule.

Disposal

Information will be securely destroyed or permanently de-identified when no longer required.

8. STUDENT INFORMATION PROTECTION

TELG recognises that student information requires additional protection.

Controls include:

- Restricted access
- Secure storage
- Need-to-know disclosure
- Parent/carer consent processes
- Media consent management

Sponsors will not receive identifiable participant information unless specific consent has been obtained.

9. INFORMATION SECURITY

TELG adopts a layered approach to information security.

Minimum controls include:

- Multi-factor authentication
- Strong passwords
- Restricted permissions
- SharePoint security controls
- Device security controls
- Regular access reviews

10. DATA BREACH MANAGEMENT

TELG will maintain a Data Breach Response Plan.

All actual or suspected breaches must be:

- Reported immediately
- Assessed promptly

- Contained as quickly as possible
- Recorded in the Breach Register

## 11. COMPLAINTS MANAGEMENT

Individuals may lodge privacy complaints regarding:

- Collection practices
- Use of information
- Disclosure of information
- Access requests
- Security concerns

Complaints will be investigated fairly and confidentially.

## 12. TRAINING AND AWARENESS

TELG personnel handling information must receive training regarding:

- Privacy obligations
- Child information handling
- Information security
- Incident reporting

## 13. POLICY REVIEW

This Framework will be reviewed:

- Every two years
- Following significant legislative change
- Following major privacy incidents
- Following substantial organisational change

## 14. RELATED DOCUMENTS

The following documents support this Framework:

- Privacy Policy
- Collection Notice
- Sensitive Information Consent Statement
- Information Privacy Procedure
- Child Information Handling Procedure
- Information Security Standard
- Data Breach Response Plan
- Records Retention and Disposal Schedule
- Photography and Media Consent Policy
- Privacy Complaint Procedure

## 15. DOCUMENT CONTROL

Document Title:
Privacy & Information Governance Framework Manual

Version:
1.0

Owner:
Greg Millican

Approved By:
TELG Board

Effective Date:
1 June 2026

Review Date:
1 June 2028

Status:
Approved

THE ENGINEERING LINK GROUP (TELG)

INFORMATION PRIVACY PROCEDURE

Document Control

Document Owner: Greg Millican
Approved By: TELG Board
Version: 1.0
Effective Date: 1 June 2026
Review Date: 1 June 2028

1. PURPOSE

This Procedure establishes the operational requirements for collecting, storing, using, disclosing, retaining and disposing of personal information held by TELG.

This Procedure supports the Privacy & Information Governance Framework Manual.

2. SCOPE

This Procedure applies to:

- Board members
- Employees
- Contractors
- Temporary personnel
- Any person handling TELG information

3. INFORMATION COLLECTION

3.1 Collection Principles

TELG will only collect information that is reasonably necessary to:

- Administer programs
- Manage registrations
- Ensure participant safety
- Meet legal obligations
- Communicate with participants and schools

3.2 Approved Collection Methods

Information may only be collected through:

- Event Espresso registrations
- Approved online forms
- Email correspondence
- Approved event documentation

3.3 Information Not Collected

TELG does not routinely collect:

- Medicare numbers
- Medicare card positions
- Medicare expiry dates
- Family doctor information
- Full residential addresses

4. COLLECTION OF SENSITIVE INFORMATION

TELG may collect:

- Medical conditions relevant to participation
- Allergies
- Dietary requirements
- Accessibility requirements

Sensitive information must:

- Be directly relevant to event participation
- Be supported by informed consent
- Only be accessed by authorised personnel

5. USE OF INFORMATION

Information may only be used for:

- Event administration
- Participant communication
- Emergency management
- Risk management
- Program evaluation
- Reporting to funding bodies in aggregated form

Information must not be used for unrelated purposes.

6. DISCLOSURE OF INFORMATION

6.1 Permitted Disclosures

Information may be disclosed to:

- Parents or guardians
- Schools
- Emergency services
- Medical personnel

- Insurers
- Legal authorities where required

6.2 Sponsors

TELG will not provide identifiable participant information to sponsors without specific consent.

Sponsors may receive:

- Aggregate statistics
- De-identified participation data

7. STORAGE REQUIREMENTS

Approved storage systems:

- SharePoint
- Microsoft 365
- Event Espresso

Information must not be stored on personal cloud services.

8. ACCESS MANAGEMENT

Access must be:

- Restricted to operational requirements
- Approved by the Policy Owner
- Removed when no longer required

9. RETENTION

Information will be retained according to the Records Retention & Disposal Schedule.

10. DISPOSAL

Electronic records must be securely deleted.

Paper records must be shredded or destroyed by secure disposal providers.

11. PRIVACY INCIDENT REPORTING

All suspected privacy incidents must be reported immediately to the Policy Owner.

12. COMPLIANCE

Non-compliance may result in disciplinary action and review by the TELG Board.

THE ENGINEERING LINK GROUP (TELG)

CHILD INFORMATION HANDLING PROCEDURE

Document Control

Document Owner: Greg Millican
Approved By: TELG Board
Version: 1.0
Effective Date: 1 June 2026
Review Date: 1 June 2028

1. PURPOSE

TELG works primarily with students aged 13–18 years.

This Procedure establishes safeguards for protecting information relating to children participating in TELG programs.

2. PRINCIPLES

TELG will:

- Act in the best interests of participants
- Protect confidentiality
- Limit access to information
- Ensure information is used appropriately

3. INFORMATION COVERED

The following information is subject to this Procedure:

- Student names
- School details
- Year levels
- Parent information
- Emergency contacts
- Medical information
- Attendance records
- Photographs
- Video recordings

4. ACCESS CONTROLS

4.1 Authorised Access

Access is limited to:

- Greg Millican
- Approved TELG personnel
- Event personnel requiring access for safety purposes

4.2 Event Volunteers

Event-day volunteers will not be provided with access to registration databases.

Volunteers may only receive information required to perform event duties.

5. EVENT DAY PROCEDURES

5.1 Attendance Lists

Attendance lists must:

- Be used only where operationally necessary
- Be secured during events
- Be collected after use

5.2 Emergency Information

Emergency contacts and medical information must:

- Be available to authorised personnel
- Be stored securely
- Be destroyed when no longer required

6. PHOTOGRAPHY AND VIDEO

TELG may photograph or record events where consent has been provided.

Personnel must verify media consent status before:

- Photography
- Filming
- Publication

7. SOCIAL MEDIA

Only approved TELG personnel may publish student images.

Images must:

- Be appropriate
- Be consistent with consent provided
- Protect participant dignity

8. INFORMATION SHARING

Child information may only be shared:

- With parents/carers
- With schools where appropriate
- With emergency services
- Where required by law

9. BREACHES

Any suspected inappropriate disclosure of child information must be treated as a privacy incident and managed under the Data Breach Response Plan.

10. REVIEW

This Procedure will be reviewed every two years or following a significant incident.

THE ENGINEERING LINK GROUP (TELG)

DATA BREACH RESPONSE PLAN

Document Control

Document Owner: Greg Millican
Approved By: TELG Board
Version: 1.0
Effective Date: 1 June 2026
Review Date: 1 June 2028

1. PURPOSE

This Plan establishes TELG's response framework for actual or suspected data breaches.

2. DEFINITION

A data breach occurs when personal information is:

- Lost
- Accessed without authorisation
- Disclosed without authorisation
- Altered without authorisation
- Destroyed unintentionally

3. EXAMPLES

Examples include:

- Incorrect email recipient
- Lost laptop
- Lost attendance list
- Unauthorised SharePoint access
- Compromised Microsoft 365 account
- Event Espresso security incident

4. RESPONSE PROCESS

Stage 1 – Identification

Any TELG representative identifying a breach must:

- Record the incident
- Notify Greg Millican immediately

Stage 2 – Containment

Containment actions may include:

- Disabling accounts
- Changing passwords
- Removing access permissions
- Recovering documents

Stage 3 – Assessment

The Policy Owner will assess:

- Nature of information involved
- Number of affected individuals
- Likelihood of harm
- Required notifications

5. RISK CLASSIFICATION

Low

Minor administrative issue with negligible impact.

Medium

Limited disclosure affecting a small number of individuals.

High

Disclosure involving sensitive information or multiple participants.

Critical

Large-scale breach or compromise of student information.

6. NOTIFICATION

Where appropriate, TELG may notify:

- Affected individuals
- Parents/carers
- Schools
- Partner organisations
- Insurers
- Legal advisers

7. REMEDIATION

TELG will implement corrective actions including:

- Technical controls
- Process improvements

- Training
- Policy amendments

8. BREACH REGISTER

All incidents must be recorded.

The register must include:

- Date
- Description
- Information affected
- Risk classification
- Actions taken
- Outcome

9. POST-INCIDENT REVIEW

All High and Critical breaches must be reviewed by the Board.

10. TESTING

This Plan should be reviewed and tested annually.

Appendix A – Breach Notification Template

Date:
Incident Number:
Description:
Information Affected:
Actions Taken:
Risk Rating:
Further Actions Required:

Approved By:
Policy Owner:
Date Closed:

THE ENGINEERING LINK GROUP (TELG)

INFORMATION SECURITY STANDARD

Document Control

Document Owner: Greg Millican
Approved By: TELG Board
Version: 1.0
Effective Date: 1 June 2026
Review Date: 1 June 2028

1. PURPOSE

This Standard establishes the minimum information security requirements for all TELG information systems, records and devices.

This Standard supports:

• Privacy & Information Governance Framework
• Information Privacy Procedure
• Child Information Handling Procedure
• Data Breach Response Plan

2. SCOPE

This Standard applies to:

- Microsoft 365
- SharePoint
- Event Espresso
- TELG-owned devices
- Personally-owned devices used for TELG business
- Email systems
- Cloud storage systems

3. SECURITY PRINCIPLES

TELG will implement controls to ensure:

- Confidentiality
- Integrity
- Availability
- Accountability

4. USER ACCOUNTS

4.1 Individual Accounts

All users must have their own account.

Shared accounts are prohibited unless approved by the Policy Owner.

4.2 Account Removal

Access must be removed immediately when:

- Employment ends
- Contract ends
- Access is no longer required

5. PASSWORD REQUIREMENTS

Passwords must:

- Be at least 14 characters long
- Contain a mixture of words and symbols
- Not contain personal information
- Not be reused across systems

Passwords must never be:

- Shared
- Written in unsecured locations
- Sent via email

6. MULTI-FACTOR AUTHENTICATION

MFA is mandatory for:

- Microsoft 365
- SharePoint
- Administrative accounts
- Any system containing participant information

7. SHAREPOINT SECURITY

TELG participant information must be stored only in approved SharePoint locations.

Access permissions must:

- Follow the principle of least privilege
- Be reviewed annually
- Be approved by the Policy Owner

8. EVENT ESPRESSO SECURITY

Only authorised personnel may:

- Access registration data
- Export participant information
- Modify registration records

Exports must be deleted when no longer required.

9. EMAIL SECURITY

Personal information must only be emailed when operationally necessary.

Before sending emails:

- Verify recipients
- Use BCC where appropriate
- Remove unnecessary personal information

10. DEVICE SECURITY

Devices used for TELG work must:

- Require password or PIN access
- Enable automatic screen locking
- Maintain current operating system updates

Lost or stolen devices must be reported immediately.

11. DATA BACKUP

TELG information stored within Microsoft 365 and SharePoint will be protected using available backup and recovery capabilities.

12. SECURITY INCIDENTS

Any suspected cyber-security incident must be reported immediately to the Policy Owner.

13. ANNUAL REVIEW

The following must be reviewed annually:

- User access permissions
- Third-party systems
- Password compliance
- MFA compliance
- Security incidents

14. COMPLIANCE

Failure to comply may result in removal of access privileges and disciplinary action.

THE ENGINEERING LINK GROUP (TELG)

RECORDS RETENTION & DISPOSAL SCHEDULE

Document Control

Document Owner: Greg Millican
Approved By: TELG Board
Version: 1.0
Effective Date: 1 June 2026
Review Date: 1 June 2028

1. PURPOSE

This Schedule establishes retention periods for information held by TELG and ensures records are retained only for as long as required.

2. GENERAL PRINCIPLES

TELG will:

- Retain records for operational, legal and governance purposes
- Dispose of records securely
- De-identify information where appropriate

3. RETENTION SCHEDULE

Participant Registration Records

Examples:
- Event registrations
- Participant details
- Parent information

Retention:
7 years

Disposal:
Secure deletion

---

Medical Information

Examples:
- Allergies
- Medical conditions
- Dietary requirements

Retention:
12 months after event completion

Disposal:
Secure deletion

---

Attendance Records

Examples:
- Sign-in sheets
- Attendance lists

Retention:
2 years

Disposal:
Secure destruction

---

Media Consent Records

Examples:
- Photo consent forms
- Video consent forms

Retention:
7 years after participant reaches age 18

Disposal:
Secure deletion

---

Incident Reports

Examples:
- Injuries
- Safety incidents
- Complaints

Retention:
7 years

Disposal:
Secure deletion

---

Privacy Complaints

Examples:
- Privacy concerns
- Access requests
- Correction requests

Retention:
7 years

Disposal:
Secure deletion

---

Board Governance Records

Examples:
- Board minutes
- Policy approvals
- Governance decisions

Retention:
Permanent

Disposal:
Not applicable

---

Financial Records

Examples:
- Invoices
- Sponsorship agreements
- Accounting records

Retention:
7 years

Disposal:
Secure deletion

---

Contractor Records

Examples:
- Service agreements
- Confidentiality agreements

Retention:
7 years after contract ends

Disposal:
Secure deletion

---

Volunteer Declarations

Examples:
- Event-day confidentiality declarations

Retention:
7 years

Disposal:
Secure deletion

4. DISPOSAL REQUIREMENTS

Electronic Records

Must be:

- Securely deleted
- Removed from active storage
- Deleted from exports and temporary files

Paper Records

Must be:

- Cross-shredded
- Destroyed by approved secure disposal methods

5. DISPOSAL REGISTER

TELG will maintain a Disposal Register recording:

- Date
- Record type
- Disposal method
- Authorising officer

6. SUSPENSION OF DISPOSAL

Disposal must cease where:

- Litigation is anticipated
- A complaint is under investigation
- An access request is active

THE ENGINEERING LINK GROUP (TELG)

PHOTOGRAPHY & MEDIA CONSENT POLICY

Document Control

Document Owner: Greg Millican
Approved By: TELG Board
Version: 1.0
Effective Date: 1 June 2026
Review Date: 1 June 2028

1. PURPOSE

TELG uses photographs and video recordings to:

- Promote STEM education
- Showcase participant achievements
- Report outcomes to sponsors
- Demonstrate program impact
- Support future participation

This Policy governs the collection, storage and publication of participant images.

2. SCOPE

Applies to:

- Engineering Link Project
- Engineering Link Roadshow
- Bridge Competition (Queensland and New South Wales)
- STEM-Sell
- Teacher professional learning events
- University partnership events

3. CONSENT REQUIREMENTS

TELG will obtain consent before:

- Photographing identifiable participants for promotional purposes
- Publishing participant images
- Sharing images externally

Consent will be obtained through approved registration processes.

4. PARTICIPANTS UNDER 18

Consent must be provided by:

- Parent
- Guardian
- Person authorised to provide consent

5. USE OF IMAGES

Approved Uses

- TELG website
- Social media
- Sponsor reports
- Annual reports
- Marketing material
- Program evaluations

6. PROHIBITED USES

TELG will not:

- Sell participant images
- Provide identifiable participant images to sponsors for unrelated marketing
- Publish sensitive personal information alongside images

7. IMAGE SELECTION

Images must:

- Reflect TELG values
- Show participants appropriately
- Maintain participant dignity
- Avoid identifying sensitive information

8. IMAGE STORAGE

Images must be stored within approved TELG systems including:

- SharePoint
- Microsoft 365

Storage on personal devices is discouraged and must be temporary only.

9. WITHDRAWAL OF CONSENT

Parents or participants may request withdrawal of consent.

TELG will:

- Remove images from future publications where reasonably practicable
- Record withdrawal requests
- Update participant records

Previously published material may not always be recoverable.

10. SPONSOR REPORTING

Sponsors may receive:

- Event photographs
- Aggregate participation data

Sponsors must not use participant images beyond approved reporting purposes without separate written permission.

11. EVENT SIGNAGE

Where photography is occurring, event signage should advise attendees that photographs and video may be taken.

12. COMPLAINTS

Concerns regarding image use may be submitted under the Privacy Complaint Procedure.

13. RELATED DOCUMENTS

- Privacy Policy
- Collection Notice
- Child Information Handling Procedure
- Information Privacy Procedure
- Privacy Complaint Procedure

14. REVIEW

This Policy will be reviewed every two years or following significant legislative or operational changes.

THE ENGINEERING LINK GROUP (TELG)

PRIVACY COMPLAINT PROCEDURE

Document Control

Document Owner: Greg Millican
Approved By: TELG Board
Version: 1.0
Effective Date: 1 June 2026
Review Date: 1 June 2028

1. PURPOSE

The Engineering Link Group (TELG) is committed to managing personal information responsibly and transparently.

This Procedure establishes a process for receiving, investigating and resolving privacy-related complaints.

This Procedure supports the:

- Privacy & Information Governance Framework
- Privacy Policy
- Information Privacy Procedure
- Child Information Handling Procedure

2. SCOPE

This Procedure applies to complaints relating to:

- Collection of personal information
- Use of personal information
- Disclosure of personal information
- Storage and security of information
- Access requests
- Correction requests
- Photography and media concerns
- Data breaches
- Any alleged breach of TELG privacy policies

3. WHO MAY MAKE A COMPLAINT

Complaints may be made by:

- Participants
- Parents or guardians
- Schools

- Teachers
- Sponsors
- Contractors
- Any individual whose information is held by TELG

4. HOW TO MAKE A COMPLAINT

Complaints may be submitted:

Email:
privacy@telg.com.au

Post:
The Engineering Link Group
Attention: Privacy Officer
PO Box 229, North Lakes, Qld 4509

Complaints should include:

- Name
- Contact details
- Description of concern
- Relevant dates
- Supporting information

Anonymous complaints may be accepted where sufficient information is provided.

5. RECEIVING A COMPLAINT

Upon receipt:

- A complaint reference number will be assigned
- The complaint will be entered into the Privacy Complaints Register
- Acknowledgement will be provided within 10 business days

6. INVESTIGATION

The Policy Owner will:

- Assess the complaint
- Gather relevant information
- Review applicable policies
- Interview relevant personnel where necessary

Investigations should be completed within 30 business days where reasonably practicable.

7. OUTCOMES

Possible outcomes include:

- Explanation of TELG actions
- Correction of information
- Removal of information
- Apology
- Additional staff training
- Policy changes
- Security improvements

8. ESCALATION

Where a complainant is dissatisfied, the matter may be reviewed by the TELG Board.

9. RECORDS

TELG will maintain a Privacy Complaints Register containing:

- Complaint reference number
- Date received
- Complainant details
- Nature of complaint
- Outcome
- Date closed

10. REVIEW

This Procedure will be reviewed every two years or following a significant privacy incident.

THE ENGINEERING LINK GROUP (TELG)

COLLECTION NOTICE

Version 1.0

The Engineering Link Group (TELG) collects personal information to administer STEM education programs, competitions and events, communicate with participants and schools, ensure participant safety, manage emergencies and meet legal and operational obligations.

Information We Collect

TELG may collect:

Participant Information

- Student name
- School
- Year level

Parent/Guardian Information

- Parent or guardian name
- Email address
- Telephone number

Emergency Information

- Emergency contact details

Sensitive Information

- Medical conditions relevant to participation
- Allergies
- Dietary requirements
- Accessibility requirements

Media Information

- Photography and media consent preferences

Why We Collect Information

Information is collected to:

- Process registrations
- Manage participation in TELG programs
- Communicate event information
- Ensure participant safety

- Respond to emergencies
- Meet insurance requirements
- Evaluate and improve programs

Disclosure of Information

TELG may disclose information where reasonably necessary to:

- Schools
- University partners
- Event venues
- Emergency services
- Medical personnel
- Insurers
- Service providers supporting TELG operations

TELG will not disclose identifiable participant information to sponsors without specific consent.

Storage and Security

TELG stores information using approved systems including:

- Event Espresso
- Microsoft 365
- SharePoint

TELG takes reasonable steps to protect information from unauthorised access, disclosure, loss or misuse.

Access and Correction

Individuals may request access to or correction of their personal information by contacting TELG.

Privacy Information

Further information regarding TELG's privacy practices is available in the TELG Privacy Policy.

Contact

privacy@telg.com.au
www.telg.com.au