1. PURPOSE

1.1. Golf Ontario is committed to protecting Confidential Information and Personal Information in its care. This includes information relating to employees, members, athletes, volunteers, and stakeholders.

1.2. This Policy establishes expectations for the collection, use, access, disclosure, and protection of Confidential Information.

1.3. This Policy supports:

1.3.1. privacy and legal compliance obligations

1.3.2. safeguarding responsibilities (including protection of minors)

1.3.3. organizational integrity and trust

2. SCOPE

2.1. This Policy applies to:

2.1.1. employees

2.1.2. contractors

2.1.3. board members

2.1.4. volunteers

2.2. Compliance with this Policy is a condition of employment or engagement.

3. DEFINITIONS

3.1. ***Confidential Information***

Confidential Information includes any non-public information relating to Golf Ontario's operations, including but not limited to:

3.1.1. financial, business, and strategic information

3.1.2. operational and program information

3.1.3. intellectual property and systems information

3.1.4. internal communications and reports

3.2. ***Personal Information***

Personal Information means information about an identifiable individual, including:

3.2.1. employees, athletes, members, volunteers, and stakeholders

3.3. ***Participant and Minor Information***

Information relating to athletes or participants, particularly minors, including:

3.3.1. registration details

3.3.2. contact information

3.3.3. performance or club membership information

3.3.4. medical or accessibility needs

3.3.5. safeguarding or incident records

3.4. ***Safeguarding Information***

Information relating to:

3.4.1. complaints, investigations, or reports of misconduct

3.4.2. suspected abuse, harassment, or rule violations

4. GENERAL PRINCIPLES

4.1. Confidential Information must only be accessed, used, and disclosed for legitimate organizational purposes

4.2. Access to Confidential Information will be:

4.2.1. restricted on a need-to-know basis

4.2.2. based on role and responsibilities

4.3. All individuals must:

4.3.1. act with discretion

4.3.2. prevent unauthorized access or disclosure

4.3.3. protect information in all formats (physical, electronic, verbal)

5. EMPLOYEE AND WORKPLACE RESPONSIBILITIES

5.1. ***Use and Disclosure***

Individuals must:

5.1.1. only use Confidential Information for authorized duties

5.1.2. not disclose information without appropriate authorization

5.1.3. not use information for personal benefit

5.2. ***Unauthorized Access ("No Snooping")***

Individuals must not:

5.2.1. access information out of curiosity

5.2.2. access records related to individuals they know without authorization

5.2.3. browse or search records without a legitimate business need

5.3. ***Workplace Conduct***

Confidential Information must not be:

5.3.1. discussed in public or unsecured settings

5.3.2. shared through unauthorized channels (e.g., personal email, messaging apps)

5.3.3. disclosed to unauthorized employees, volunteers, or third parties

6. PROTECTION AND SAFEGUARDS

6.1. All Confidential Information must be protected using appropriate safeguards, including:

6.1.1. secure systems and approved platforms

6.1.2. password protection and device security

6.1.3. secure storage of physical records

6.2. Individuals must comply with:

6.2.1. Computer & Software Policy

6.2.2. AI Use Policy

6.2.3. Data Management and Compliance Policy

6.3. Confidential Information must not be:

6.3.1. stored on unauthorized systems

6.3.2. transferred outside approved tools or platforms

7. TECHNOLOGY, SYSTEMS, AND MONITORING

7.1. Use of organizational systems must comply with:

7.1.1. Computer & Software Policy

7.1.2. AI Use Policy

7.2. Confidentiality obligations apply equally when:

7.2.1. working remotely

7.2.2. attending events or travel

7.2.3. using organizational devices or systems

7.3. Employees are subject to electronic monitoring in accordance with the Electronic Monitoring Policy.

7.4. Confidentiality does not eliminate or override monitoring practices necessary for security, compliance, and investigations.

8. LEGAL, SAFEGUARDING, AND AUTHORIZED DISCLOSURE

8.1. Nothing in this Policy prevents an individual from making a report or disclosure that is:

8.1.1. required or permitted by law

8.1.2. necessary to protect health, safety, or wellbeing

8.2. Individuals may disclose Confidential Information where appropriate to:

8.2.1. child protection authorities (CAS)

8.2.2. law enforcement or emergency services

8.2.3. regulatory or sport integrity bodies

8.2.4. legal counsel or investigators

8.3. Confidentiality must not interfere with safeguarding obligations, including:

8.3.1. reporting suspected abuse or misconduct

8.3.2. participating in investigations

8.4. Where disclosure is appropriate under this section, prior internal approval is not required.

9. BREACH REPORTING

9.1. All individuals must immediately report:

9.1.1. unauthorized access or disclosure

9.1.2. lost or stolen information or devices

9.1.3. suspected privacy or data breaches

9.2. Reports must be made to the Privacy Officer or designated contact

9.3. Failure to report a breach may result in disciplinary action.

10. RECORDS MANAGEMENT AND RETENTION

10.1. Confidential Information must be retained, stored, and destroyed in accordance with the Records Retention Policy

10.2. Individuals must:

10.2.1. follow secure handling practices for records

10.2.2. ensure proper destruction when authorized

10.3. Confidential Information must not be:

10.3.1. kept longer than necessary

10.3.2. retained outside authorized systems

11. INTERPRETATION AND GUIDANCE

If an individual is unsure whether information is confidential, or whether disclosure is permitted, they must seek guidance from the Privacy Officer or appropriate leadership

12. COMPLIANCE AND ENFORCEMENT

12.1. Compliance with this Policy is mandatory.

12.2. Failure to comply may result in:

- 12.2.1. disciplinary action up to and including termination
- 12.2.2. additional legal or regulatory consequences where applicable

13. Related Policies

13.1. This Policy must be read in conjunction with:

- 13.1.1. Privacy Policy
- 13.1.2. Code of Conduct & Ethics Policy
- 13.1.3. Data Management and Compliance Policy
- 13.1.4. Records Retention Policy
- 13.1.5. Computer & Software Policy