GOAL ONLINE PRIVACY POLICY

Policy Purpose

1) To illustrate circumstances in which GOAL would be granted permission to access information or content in use by GOAL’s website or IT resources.
2) Ensuring the continued confidentiality, integrity, security, functionality, and availability of GOAL’s systems
3) Providing appropriately de-identified data for institutionally approved research projects
4) Respond to valid legal requests
5) Here to protect the trust between the user and GOAL

While not impeding on user’s rights, GOAL’s policy seeks to provide an online environment that balances the individual’s freedom and privacy with the need for access by persons other than the account holder.

Policy Statement

*This policy covers

- GOAL data and other GOAL associated files on personally owned devices
- GOAL-owned computers assigned to employees or groups used in support of job functions
- GOAL-owned systems/devices, or systems/devices managed by GOAL on behalf of affiliated organizations

GOAL is the sole owner of the information collected on the website. We have no intention of selling or renting out information collected to anyone

Access by technicians and administrators that requires authorization

Except for monitoring of activity and accounts of individual users of GOAL’s IT Resources when the user has voluntarily made them accessible to the public, any access to the contents of communications or electronically stored wire and electronic communications and information employing IT Resources permitted under this policy must, in addition to any requirements specified herein, be authorized as follows:

1. The official designee of the Office of the Vice President for Information Technology shall have made a written finding prior to such access that:

   (a) The access is reasonably required in order to protect GOAL’s Interests;

   (b) Authorizes the requested access and specifies the scope and conditions of any permitted access. These written findings shall be maintained by the Office of the Vice President for Information Technology.

2. Notwithstanding the foregoing, the Vice President for Information Technology or his or her designee may authorize access in the event that he or she reasonably determines that:
(a) There exists an emergency that materially threatens GOAL’s interests,
(b) That emergency access is reasonably required in order to protect GOAL’s Interest
(c) He or she specifies the scope and conditions of any permitted access.

Any access permitted hereunder shall be the minimum access required in order to protect GOAL’s Interests.

In all cases, technicians and administrators who receive requests from law enforcement or other outside agencies seeking access to computer accounts, files, or network traffic of an IT Resource user shall forward such requests to the appropriate and responsible GOAL representative, in accordance with applicable GOAL policy. In all cases, technicians and administrators will obtain written documentation of any requests made before accessing or permitting access to an individual's electronic information resources.

**Method of Enforcement**

- Security tools designed to locate security flaws in equipment connected to IT Resources
- Network monitoring hardware and software that capture the contents of packets traversing the network
- A technician or administrator accessing information covered by this policy shall make reasonable efforts to report such access to the affected individual prior to that access

**Rationale**

- This policy seeks to balance individual freedom and privacy with the need for access by persons other than the account holder when necessary to serve or protect other core values and operations within GOAL or to meet a legal requirement

**Scope**

- This specific policy applies to all users of the GOAL website and technology resources.
- Online customers using the GOAL website
- All employees, full time and part time
- Interns; guests; on-sight customers
- Anyone who interacts with GOAL I.T. systems or resources

**Intended Outcome**

- Seek to create, maintain, and protect the privacy of electronic information on its IT Resources
- To protect GOAL and all authorized users
- To protect GOAL’s core values
Consequences of Violation

Violations of this policy or any other of GOAL’s policies or regulations may result in the revocation or limitation of IT Resource privileges as well as other disciplinary actions or may be referred to appropriate external authorities.