Go Out and Live (GOAL)
Privacy for Electronic Information

Policy Purpose, Rationale, and Intended Outcome:
The purpose of this policy is to outline situations in which GOAL may access content or electronically stored communications and information to ensure freedom and privacy for the user, while preserving the core values of GOAL and meeting legal requirements. The intended outcome of this policy is to balance the freedom of privacy for users of GOAL IT Resources, while maintaining security and preserving core GOAL organizational values and meeting legal requirements.

Scope:
This policy covers faculty, staff, and any and all individuals using any GOAL IT Resources and all uses of such IT resources. This includes:

- Data, email, and voice mail stored on, encrypted on, or in transit to or from individual computer or voice mail accounts on GOAL-owned systems or devices;
- GOAL-owned computers assigned to a specific individual or group for use in support of job functions;
- Data and voice communications to, from, or between any IT Resources, including, but not limited to, the devices listed above.

Policy Statement:
1) A technician or administrator shall access data as outlined above in the following cases:
   a) Upon receipt of a voluntarily written authorization from the individual to whom the account or device or communication has been assigned or attributed; or
   b) Upon receipt of a written authorization from the appropriate Manager, Director, or Officer (or equivalent) for situations where there is reasonable belief that the individual to whom the account or device is assigned or owned has used, is using, or intends to use the services or devices in question provided to engage in illegal activities or violations of GOAL policy; or
   c) Upon receipt of a directive from the Office of General Counsel confirming that access is legally required under the terms of a valid subpoena, warrant, or other legal order or GOAL policy; or
   d) Upon receipt of a written authorization (which may be preceded by verbal authorization) from the appropriate Manager, Director, or Officer (or equivalent) approving access after concluding that access is necessary to address an emergency or to avoid or minimize exposure of the organization to substantial risk of harm or liability.

Consequences of Violation:
This policy shall be enforced on a combination of a report and security audit basis. Violation of the policy as outlined above is subject to the consequences outlined below:

- Should a technician, administrator, or other individual access information without proper authorization as outlined in this policy, the individual is subject to disciplinary review and action up to and including termination.
- Should the aforementioned individual violate this policy in a manner that violates federal, state, or local law, the individual is subject to the disciplinary actions described above and immediate report to the appropriate law enforcement body.