

## Computer Services

The Computer Center offers accounts (including email accounts) and various computer laboratories for St. Andrews students. The Computer Network is owned solely by St. Andrews Presbyterian College.

### Acceptable Use of Information Technology Resources

Technology should not be used in a manner that infringes upon an individual's right to privacy. The following restrictions are to protect your privacy, as well as the privacy of others. Account holders are prohibited from:

1. Using computer or network services in a way that violates copyrights, patent protections or license agreements;
2. Gaining unauthorized access to information that is private or protected, or attempting to do so;
3. Attempting to identify passwords or codes, interrupting security programs, or attempting to do so;
4. Monitoring or tampering with another person's e-mail;
5. Reading, copying, changing or deleting another person's work;
6. Using another person's user id/password, or allowing others to use yours; and,
7. Attempting to gain system and or network privileges to which you are not entitled.

### Respectful Exchange of Ideas and Information

Computer systems and networks allow for a free exchange of ideas and information. This exchange serves to enhance learning, teaching, critical thinking and research. While the constitutional right of free speech applies to communication in all forms, we encourage civil and respectful discourse. St. Andrews policy and local, state and federal law do prohibit some forms of communication, to include:

1. Obscenity;
2. Defamation;
3. Advocacy directed to incite or produce lawless action;
4. Threats of violence;
5. Disruption of the academic environment;
6. Harassment based on sex, race, disability, or other protected status; and,
7. Anonymous or repeated messages designed to annoy, abuse or torment.

### Personal Responsibility

Each individual who obtains a computer/e-mail account, or uses the computers and network resources made available by St. Andrews, must understand that he/she is accountable for the guidelines set forth in this document. In addition, each account holder assumes responsibility for:

1. Protection of his/her password;
2. Reporting any breach of system security;
3. Reporting unauthorized use of his/her account; and,
4. Changing his/her password on a regular basis.

### Authority

Computer Services may access users' files for the maintenance of networks, computers and storage systems. In all cases, an individual's expectation of privacy will be respected to the greatest degree possible. Computer Services staff may also routinely monitor and log usage data, such as network connection times, CPU and disk utilization for each user, security audit trails, and network loading. Data collected may be reviewed and further investigated should evidence of violation of policy or law occur.