GOAL Academy
Information Protection Acceptable Use Policy

Section: C: General School Administration

Policy Number: C-2

Policy Name: Information Protection Acceptable Use Policy

Approval Authority: Board of Directors

Responsible Executive: Chief Information Officer

Responsible Office: Chief Information Officer

Originally Issued: 7/31/2018

Revisions: 7/29/2025

1. Policy Statement - GOAL Academy's Information Protection framework sets out general guidelines for handling and communicating organizational information. In conjunction with the information valuation and storage policy, this document is meant to provide guidance for employees on how information will be treated.

This Acceptable Use Policy (AUP) applies to the use of all information and IT equipment by GOAL Academy staff (including temporary workers, subcontractors, business partners, and staff seconded or contracted from other organizations). All staff should be aware of their legal obligations and internal policy in respect of information handling.

Any breach of such obligations may constitute a breach of the law and may also be dealt with through local disciplinary processes which may result in dismissal or criminal prosecution.

2. **Reason for Policy** - The purpose of this policy is to provide staff with clear guidance on the appropriate, safe, and legal way in which they can make use of IT equipment at GOAL Academy. Staff need to be aware of the compliance required with this policy and GOAL Academy's commitment to comply with the business requirements that all reasonable organizational and technical measures are taken to safeguard its data.

All employees are expected to have knowledge of at least the portions of this document that are directly related to their role within the organization.

3. Who Should Read This Policy

All members of the GOAL Academy community

4. Related Documents

Board Policy C-4 Artificial Intelligence Acceptable Use Policy

5. Contacts: Chief Information Officer

6. POLICY

1. Duties / Responsibilities

Legal and Compliance

The primary responsibility for determining changes to the AUP belongs to the Chief Information Officer for GOAL Academy, with further inputs from the GOAL Academy Leadership Team. As such, this person is the executive responsible for managing organizational risk with respect to Information Technology and Information Security.

Chief Information Officer/IT Department

The Chief Information Officer ("CIO") is responsible for ensuring any of GOAL Academy's technical systems can meet our risk management needs as defined by compliance rules. All projects that use or require access to information handling systems (ECM, file shares, CRM, website, ERP, etc.) must be approved in writing by the CIO or designee. The CIO and the IT department are responsible for ensuring that the project or device is able to comply with all of the security requirements within this policy.
Compliance also requires that staff are aware of their responsibilities, so the CIO and IT staff are responsible for ensuring any training needs for IT equipment introduced by the department are met.

All Staff

All GOAL Academy staff, (including temporary, contract, subcontract, business partners, and honorary), who have access to and make use of IT equipment and GOAL Academy IT systems are responsible for using it in accordance with the rules within this policy. In particular, all staff must ensure that they use systems in such a way that they ensure student and staff confidentiality is maintained.

2. Information Quality and Valuation as an Asset

~~Staff will be provided~~ An appointed member of the IT department will provide staff, at the time of hire, yearly, and as otherwise directed or requested with clear guidance and procedures regarding:

- How to use systems appropriately to ensure that information that is recorded is accurate, up to date, and complete.
- How to access help facilities.

- Clear, current, and relevant definitions of information required.

These procedures shall be available to all staff at the moment of account creation and at request.

All Staff shall ensure that there is a clear, regular process of review for the quality of information captured, including the use of feedback from external sources and from validation reports. Audit trails will be used to identify where any identified errors have occurred. ---- mechanisms are built into each system to rectify issues and ensure that consequent training needs are built into refresher training for appropriate individuals.

3. Communication

Social media

GOAL Academy, through the Communications Department uses LinkedIn, X (formerly known as Twitter), Facebook, TikTok, Instagram, Snapchat, and other social media types to enhance both its school visibility and image. Employees of the Communications Department are expected to use these media types in a manner that is consistent with the GOAL Academy Social Media Acceptable Use Policy. Other GOAL Academy employees may not use personal social media accounts to represent, post on behalf of, or communicate any school position of any kind. Employees may also not use personal social media accounts to communicate with GOAL Academy students or families.

Instant Messaging

Instant messaging is available for internal business-related use through IT Department approved methods.

Personal use of email

It is permissible for staff to send and receive email at work for incidental personal purposes, provided that it adheres to the specifications provided herein, does not involve GOAL paid work time, or use for profit. Personal email should not add a significant burden to GOAL Academy's IT systems. The size of messages, the frequency with which they are sent, and the number of recipients (within GOAL Academy) should not be excessive, and may be monitored to ensure system performance. GOAL Academy has the final decision on what constitutes excessive use. Staff must act in accordance with their manager's local guidelines. It is not permitted to write or present views on behalf of GOAL Academy unless you are authorized in writing to do so.

External email

No personally identifiable information or records should be transmitted via email to any external account. This includes personal accounts of GOAL Academy employees. Email queries received from members of the public should always be responded to in writing, not electronically, as it is not possible to be certain that the sender is who they appear to be, or that the message will be read by them.

Email attachments

Users should treat attachments that have been sent unsolicited with extreme caution, especially if the sender is unknown. Viruses are often sent this way. If you are not sure what an attachment is for, or why someone has sent it to you, you should not open it and seek advice from the IT Helpdesk. To intentionally introduce files which cause computer problems is strictly forbidden and could be prosecutable under the Computer Misuse Act of 1990.

Sending to a distribution list

Do not send or forward email to any large group of staff unless there is a genuine business related reason for them to read it. GOAL Academy employs a moderation system for emails sent to all staff and other certain groups. Do not advertise by email. Do not circulate warnings about any virus risk but consult with the IT Helpdesk. When sending email to external addresses, consider the possibility that this action may inadvertently reveal email addresses to third parties.

Automatic forwarding of email

You should not set up auto-forward rules from your mailbox unless directed to do so by your supervisor. You must set an out of office message for your mailbox if you will be out of the office for over 24 hours.

Forging email messages

Forging an email (or any other electronic message), sending email from any account other than your own without permission, and any unauthorized accessing another staff account may be treated as fraud.

Offensive email

GOAL Academy employees are prohibited from using the email system to transmit offensive, harassing, or discriminatory content; engage in personal business or commercial activities; distribute chain letters, spam, or unauthorized mass mailings; encourage, distribute, recruit, or otherwise use the system for religious or outside group purposes; share confidential or sensitive information, including student records, without proper authorization; or access, download, or distribute malicious software or unlicensed content. Email accounts must not be used to impersonate others or misrepresent the organization.

Email will not be used for intentional receipt and/or distribution of offensive, obscene, or pornographic material. There is a legal requirement for all staff to report any computer crime involving child pornography to the police. If you receive an email connected with child pornography, seek advice from your manager immediately so that GOAL Academy can take appropriate preventative action.

If you receive any pornographic or offensive email, do not open it or print it. Fill in an incident form (located at http://helpdesk.goalac.org) and let the Chief Information Officer and your immediate supervisor know of the incident so that appropriate action may be taken.

If you receive an email containing sexually or racially abusive or discriminatory phrases or material, seek advice from your manager or the Human Resources department.

No member of staff is permitted to distribute email that contains offensive material. To do so is considered a serious breach of GOAL Academy security and may result in dismissal. Offensive material is defined by GOAL Academy's Employee Handbook or other Human Resources published documents and includes hostile text or images relating to gender, ethnicity, race, sex, sexual orientation, religious or political convictions and disability. This list is not exhaustive. Other than instances which demand criminal prosecution, GOAL Academy is the final arbiter on what is or is not offensive material, or what is or is not permissible use of email.

4. Taking IT Equipment Offsite

Any PC, laptop, printer, or mobile device owned or provided by GOAL Academy is subject to the same conditions of use whether used at home or in the office.

Users should take all reasonable care and precautions to ensure safe transport and storage when moving equipment between home or other remote locations and work, keeping it locked and out of sight.

Users may be held fully or partially liable for any loss, damage, or theft occurring to GOAL Academy IT equipment whilst in their care. You are within your rights to refuse to take information and equipment offsite if you feel circumstances mean that you are not able to protect it adequately.

All GOAL Academy confidential documentation, whether in paper or data format should be stored in a secure area of users' homes or the remote location they are working from.

For further guidance, staff may contact the IT Department.

5. Personal IT Equipment

The use of any customer, student, or HR related identifiable information on personally owned equipment is strictly forbidden.

GOAL Academy business and student information (such as spreadsheets, plans, and reports etc.) may not be used or stored on personally owned equipment.

To restrict the possibility of viruses being transmitted to the organizational computers and

network, staff must not use their own computer for work-related activities.

Personal mobile devices may not be synchronized with work email for calendar, contact, and email purposes where permitted by email policies and guidance.

For further guidance, staff should refer to GOAL Academy Acceptable Usage Policies ("AUP") on mobile information handling and computing policy.

In circumstances where the organizational resources do not meet the needs of end users, project or access requests can be submitted through normal IT channels.

6. Monitoring Compliance

The effectiveness of this policy will be ensured by way of a quarterly review of reports as part of the Information Technology Security Committee's meeting. It is expected that IT Helpdesk personnel will record any incidents showing non-compliance. A database is maintained by the IT Helpdesk to allow for review of any patterns.

New members of staff are given a copy of the AUP on recruitment to GOAL Academy.

Members of GOAL Academy who oversee certain content and information may also be asked to confirm that this policy is effective within the departments and information they oversee. Results of audits of local IT systems will be reviewed to ensure that a picture is obtained of the extent to which the AUP is clearly understood by all staff.

Local experts and departments are expected to audit their own practices from time to time to measure compliance with this policy or to comply with future GOAL Academy requirements.

7. General Usage

Staff will only access IT systems provided to them for duties in connection with their employment or engagement and in accordance with their terms and conditions of employment or equivalent. Access to some applications and information sources will be routinely recorded and/or monitored for this purpose.

Any changes to information access designed to expand use or change the storage location of information sources requires written approval from the IT Department and the department overseeing the information.

GOAL Academy's systems must not be used for the creation, transmission or deliberate reception of any images, data or other material which is designed or likely to cause offense or needless anxiety, or is abusive, sexist, racist, defamatory, obscene, or indecent. When communicating electronically, staff are expected to conduct themselves in an honest, courteous, and professional manner.

GOAL Academy's systems must not be used for private work, or for storage of personal non-work-related files, except where prior arrangements have been agreed with GOAL

Academy. At a Principal, Director, or Executive Directors approval, an employee may use GOAL's systems outside working hours with appropriate payment for consumables for work unrelated to the employee's employment duties.

Staff may not use GOAL Academy's IT facilities for commercial activities. This includes but is not limited to, advertising or running any sort of private business.

Use of GOAL provided internet during GOAL work time for commercial activities other than in the conduct of GOAL Academy business is prohibited.

Use of GOAL provided internet and other GOAL Academy owned IT equipment for political or religious activities is prohibited.

Staff may not use GOAL Academy's IT systems or facilities for advertising or fundraising for commercial or charitable organizations not directly connected with or sanctioned by GOAL Academy.

It is the responsibility of all staff to ensure that computer systems and facilities and the data, which is accessed through them, are safe and secure. Systems should be placed in an area where it is not likely to be damaged and where the content of screens cannot be read by unauthorized people.

All staff will ensure that any print-outs or other outputs from GOAL Academy's systems are appropriately protected and disposed of when no longer needed. Print-outs may not be copied, removed from the workplace, or shared with others without proper authorization.

Any member of staff who suspects or is made aware of a security breach must immediately alert the IT Helpdesk, who will initiate investigation procedures. Depending on the breach scenario, investigations will be carried out by the GOAL Academy Chief Information Officer with inputs from other members of the GOAL Academy Leadership Team as necessary. If warranted, the findings will be subsequently reported to GOAL Academy's Leadership Team for further action and direction.

Deliberate activities with any of the following consequences (or potential consequences) are prohibited:

- Corrupting or destroying other users' data.
- Using systems in a way that denies service to others (e.g. overloading the network).
- Wasting staff effort or computing resources including staff involved in the support of those resources.
- Gaining access to systems which you are not authorized to use.

GOAL Academy reserves the right to suspend or remove access, temporarily or permanently from any user suspected of or under investigation for misuse.

8. Information Security

Authorization

On request, the IT department will provide each member of staff with a personal username and password. These must be used to gain access to any GOAL Academy computer. Usernames and passwords will only be issued when authorized by an appropriate authorized signatory, and when identity checks have been completed satisfactorily.

Before a password is issued, staff must complete the appropriate authorization/registration forms that will request the user to read, understand, and abide by the terms of this overarching Acceptable Use Policy.

Passwords

The IT department will endeavor to provide all PCs with secure access facilities. Access to databases or systems containing important, sensitive, and/or confidential information will be restricted to those staff who require access as part of their job function. These may be protected by additional security controls.

Where passwords are used, users will be able to select and change their own password by using a minimum of 8 characters (all user passwords must contain a capital letter, a lowercase letter, a number, and a special character). The only exceptions to this are where the security controls on older computers are not available or system configuration passwords are not tied to a particular user.

You should not leave any computer unattended without either logging out or activating a password-protected screensaver. Where a previous user has left their access open, new users must log out from that session first.

Users should not add additional password or security measures to any PC or files without first consulting with the IT department.

Attempting to remove or bypass any security access on any GOAL Academy computers is strictly forbidden.

Passwords are issued for personal use only. GOAL Academy staff are forbidden from sharing password or other credentials with other staff unless expressly authorized by the Chief Information Officer. Users are required to protect their usage against loss, damage, or theft and against possible misuse by others. If a breach of security is recorded, the burden of proof will be with the registered user to show that they are not responsible for the breach.

Users should report any known or suspected breaches of information security to the Chief Information Officer or IT Helpdesk for any necessary action to be considered and undertaken.

9. Confidentiality & Privacy

All staff are responsible for ensuring that confidential information is stored securely and that appropriate confidentiality is maintained when handling information.

10. Privacy of Documents

Monitoring

GOAL Academy reserves the right to monitor the use of its information and communication systems where permissible by law. Routine monitoring may be undertaken to check efficiency, capacity, and appropriate use. If unacceptable activity is taking place, as defined by GOAL Academy, disciplinary action may be imposed in accordance with GOAL Policy.

Any investigation required as a result of monitoring or identified by other means (e.g. reports from other staff members) will be conducted in line with GOAL Academy's appropriate Human Resource Policy.

A copy of every document stored on GOAL Academy's systems may be archived by the IT department. These may be used for investigation of unlawful acts, system failure, or system misuse. These include a copy of every email and instant message sent and received and a full history of all internet access. Statistics on the source, destination, size and number of emails sent and received by each user may be recorded, and archived.

The IT department will purge records as prescribed by the Document Retention Policy. Such purges will not be conducted on information that is required to be archived or stored for a longer period of time, or as any compliance matter directs. In addition, all records will be governed by the appropriate Retention Policy.

Disclosure

Access to read the document archives will only be granted to staff responsible for investigating system failure or system misuse, and then only to look at information as necessary to repair or protect the systems or to investigate use that may be in contravention of this AUP.

Document files, web browsing logs, email or voicemail messages, however confidential or damaging, may have to be disclosed in court proceedings or during internal investigations if relevant to the issues being investigated.

Access to a user's personal documents either stored or held in an email mailbox will only be granted to another user if a written request, with appropriate reasons is received from the appropriate department manager or executive.

11. Copyright

Infringement of copyright by copying or transmitting copyright material without permission

of the copyright holder ("fair use" notwithstanding) is strictly forbidden. The GOAL Academy name/logo may be used only for official GOAL Academy documents and must be used in accordance with the school's identity guidelines.

12. Disposition and Retention of Information

The IT department schedules fileserver backups to enable recovery from any system failure. Please follow GOAL Academy's standard practice of moving documents to the appropriate locations based on document accessibility need.

If you do not have access to save your work to a GOAL Academy fileserver or cloud storage drive, it is essential that you regularly copy any important work either to disk, a backup device, or another machine. The IT Department does not maintain backups for information stored locally on a user's computer.

Backup copies (including disks) must be stored in a secure area, e.g. fireproof safe.

If access is given to an email account and it is not used for a four-week period, the account may be disabled. To re-enable the account, users must complete the appropriate documentation and forward it to the IT Helpdesk; the request may be discussed prior to reactivating any access. For employees placed on administrative leave the request for access will come from the Human Resource department.

Employees placed on administrative leave may have their access to GOAL equipment and platforms restricted.

Accounts not used for 3 months (without prior warning) may be deleted under the assumption that the employee has left the organization. The IT department will make every reasonable effort to verify this with Human Resources.

If you change job role, you should ensure your computer access has been amended appropriately.

If you change job role, you should hand-over all relevant personal files and email messages to your line manager.

13. Leaving GOAL Academy Employment

Upon termination of employment from GOAL Academy, staff accounts will be suspended immediately. IT will follow published HR notifications of last day worked. Employees are expected to leave in place GOAL Academy assets, such as email or documents.

Employees must turn in all IT equipment to the IT department or their immediate supervisor.

Employees are not entitled to copies or backups of contacts, emails, documents, student records, or any other information accessed or used on GOAL Academy owned networks.

14. Virtual Networking

Remote control software is used by the IT department to connect and take control of a PC remotely. Access to this software is only permitted by IT Staff. You should not attempt to use any remote control software, nor allow external users or support staff to use it without the express permission of the IT department.

15. Use of the Internet for Non-Work Purposes

Access to the Internet is primarily provided for work-related purposes.

Reasonable personal use is permitted provided this does not interfere with the performance of your duties or adversely affect system performance. GOAL Academy has the final decision on what constitutes excessive use. You may access some services (e.g. personal email or online banking) provided these are within the boundaries of incidental personal and acceptable use. GOAL Academy cannot guarantee the privacy of staff accessing these facilities from work.

Personal access to the Internet can be limited or denied by your manager. Staff must act in accordance with their manager's local guidelines.

The IT department has the right to withdraw internet access from any user and globally ban access to any site as appropriate, without warning.

Unless specifically authorized, no member of staff may post messages under GOAL Academy's name or trademarks to any newsgroup or chat room.

Unless specifically authorized by the IT department, no member of staff may publish a website under the name of GOAL Academy or featuring its logo or trademarks.

GOAL Academy will not accept liability for personal legal action (e.g. libel) resulting from staff misuse of the Internet.

Access to file downloads will be restricted as necessary by IT to ensure system security.

GOAL Academy reserves the right, consistent with State, Federal, and local law, to monitor all internet accesses, including but not limited to email and web access. No member of staff should consider information sent/received through the Internet as his/her private information.

No member of staff is permitted to access, display, or download from internet sites that hold offensive material. To do so is considered a serious breach of GOAL Academy security and may result in dismissal.

Personal/employee identifiable data must not be published in any way on the Internet without the express consent of each and every individual concerned.

16. Licensing

Accessing and manipulating information

All software must be purchased, installed, and configured by the IT department, this includes all software packages, software upgrades, and add-ons - however minor. It also includes shareware, freeware, and any items downloaded from the Internet. Under no circumstances should any software be purchased or installed without the explicit agreement of the IT department.

Do not violate the license agreement by making illegal copies of GOAL Academy software.

Software not licensed to GOAL Academy must not be loaded onto GOAL Academy computers. Software licensing will be arranged and recorded by the IT department as part of the procurement and/or installation process.

You are not allowed to download software from the Internet or install from CD or disc without IT department authorization. Any unlicensed software found on a GOAL Academy PC or laptop will be automatically deleted or disabled, and disciplinary action may be taken.

Using personal software for business purposes

The use of any software package to access, modify, or analyze GOAL Academy's data for either work or personal purposes is forbidden without prior approval. The expectation by the IT department is that this use constitutes a short-term pilot.

There should be no expectation that long-term use will be permitted or that GOAL Academy will pay for personal software. Any information created or used must be stored appropriately based on the storage and retention rules that govern that information source.

17. Artificial Intelligence (AI) Use

The use of Artificial Intelligence (AI) tools and systems within the organization must align with ethical, legal, and security standards. Employees are prohibited from using AI technologies to generate or disseminate misleading, discriminatory, or harmful content. AI tools must not be used to process or analyze confidential, proprietary, or personally identifiable information (PII) without explicit authorization. All AI-generated outputs used in decision-making must be reviewed by a human to ensure accuracy and fairness. The use of generative AI (e.g., chatbots, image generators, code assistants) must be approved by IT and comply with data protection and intellectual property policies. Misuse of AI tools may result in disciplinary action.

Please refer to GOAL Academy Board Policy C-4, Artificial Intelligence Acceptable Use.