Deerfield Academy
Information Technology Services

revised July 2022

WORKING INFORMATION SECURITY POLICY

PURPOSE

The **Working Information Security Policy (WISP)** is an umbrella document that outlines information and data security processes, policies, and practices that protect Academy data, and ensure compliance with applicable laws and regulations.

The goals of Information Security are generally distilled into three main concepts:

- Security: Ensuring that only authorized users are given access to data and services provided by Deerfield Academy through technically appropriate means.
- Integrity: Ensuring that the information maintained and provided by Deerfield Academy and the institution's information services is accurate and obtained from authorized, reliable, and verifiable sources.
- Availability: Ensuring that the information and services that Deerfield Academy provides are available to those who need them, when they need them.

The purpose of this document is to outline the ways that Deerfield Academy is committed to meeting these goals in relation to management of the data and information services provided to the Academy community.

SCOPE

This document addresses the security of all data, regardless of form or storage medium. This means that it does not matter whether the information is stored electronically, in paper records, or otherwise; *this policy applies regardless.* However, the classification of data is important to how we manage its security. We divide information into three categories:

A. **Confidential and/or Personally Identifiable Information (PII)** is any information that is in one or more ways protected by law. PII is a specific subset of confidential information described by Massachusetts Law as – *first name and last name or first initial and last name in combination with any one or more of the following data elements that relate to such resident: (a) Social Security number; (b) driver's license number or state-issued identification card number; or (c) financial account number, or credit or debit card number, with or without any required security code, access code, personal identification number or password, that would permit access to a resident's financial account; provided, however, that "Personal information" shall not include information that is lawfully obtained from publicly available information, or from federal, state or local government records lawfully made available to the general public.* Any information in this category must be protected by the highest level of security and treated with the utmost care. Only specifically authorized users with a demonstrated business need will be allowed access to information in this category, and no information in this category should ever be communicated or shared with anyone not explicitly authorized by the information owner to have the information.

B. **Sensitive Information** is information whose unauthorized disclosure is not a per se violation of an expressed law or regulation, but may be damaging to our students, employees, alumni or Deerfield Academy's reputation if communicated to the wrong parties, and thus requires a higher degree of security and care than public information. Sensitive information may be commonly available to certain groups or members of the Deerfield Academy community for a specific business purpose, but should be restricted from general distribution. An example of sensitive information is the contact information for students, parents, or alumni.

C. **Public Information** is information that does not require a particular level of protection. We do our best to ensure that this information is accurate and represents the interests of the institution and community, but do not actively protect it by administrative action or policy. An example of public information is our Academy Calendar and our Course Catalog.

Generally, any information not classified as Confidential or Sensitive is considered Public. If there is ever any question about which classification applies to a set of data, the information should be treated as Confidential until the question is resolved.

MAINTENANCE

Security is an ongoing process, and accordingly, this document is a living document. Regular review and updates will be necessary to ensure that the information the WISP remains accurate and current. This includes the policies referenced below that comprise the foundation for the WISP.

POLICIES AND PROCEDURES

A. Access

1. Access to all electronic information systems on campus is provided by restricted authentication of each employee or authorized user. The sharing of logins, passwords, or any other credentials between people for ANY REASON is prohibited. Shared accounts are only provided on an exceptional basis, subject to authorization by the Director of ITS.
2. All passwords/PINs on employee accounts are required to have a minimum level of strength/complexity including at least fifteen characters and both letters and numbers.
3. Because login credentials provide access to secure information, they may only be communicated via secure means. Access credentials may not be sent to a user via unencrypted email.
4. Access to Confidential or Sensitive non-electronic information shall be restricted by physical security mechanisms such as locking file-cabinets.
5. Access to Confidential and Sensitive information that is stored electronically is restricted by system permissions, which are granted by a member of the ITS staff. Some permissions are granted to individuals, while others are granted to groups of people with a shared business role or need. All requests for access or changes in permissions should be submitted to the ITS Help Desk in writing, and approved by the designated data owner and/or supervisor.
6. An employee's access to the Academy's electronic information resources will be revoked by ITS upon receipt of an HR termination notice, and in accordance with termination processing protocols. The Academy's office of Campus Safety and Security will work with HR to restrict physical access to non-electronic data.

B. *Protection from Unauthorized Access and/or Modification*

1. All Confidential data should be encrypted when transmitted over open channels. It should not be transmitted electronically via any protocol that is not considered secure. This means that:
   a. Confidential information is never to be sent via un-encrypted email to anyone.
   b. All information services that transmit Confidential and/or Sensitive data must use an industry-accepted encryption protocol to prevent unauthorized access during transmission.
   c. Confidential information may not be stored on any cloud-hosted system or service without prior approval from ITS.

   d. Off-campus access to secure Deerfield Academy resources is restricted to approved employees via secure and authenticated VPN access.

   e. All on-campus wireless networks that provide access to information systems storing Confidential or Sensitive data are encrypted and require authentication for connectivity. Publicly accessible "open" wireless networks may not be used to access any of these secure resources.

   f. If a method of secure transmittal is required for an authorized business purpose, the ITS department should be consulted for an appropriate a solution.

2. All non-electronic records containing Confidential information must either locked up or under the direct supervision of an authorized person at all times.

3. Authentication logs, which record successful authentications for Deerfield's ERP system (Banner) and employee/student/parent portal (DAinfo) are retained for a minimum of 30 days.

4. All third-party vendors that access or process confidential and/or sensitive information, must comply with the information security policies of Deerfield Academy and applicable laws. Academy departments should notify ITS of any agreements with such vendors, and should participate in a joint review of the vendor's data handling policies and practices.

5. All paper records containing confidential and/or sensitive information should be shredded before being disposed of.

6. All electronic devices that store confidential and/or sensitive information must be erased or destroyed before disposal.

7. Unless otherwise provided in accordance with this policy, mobile devices (laptops, cell phones, etc.) may not be used to store unencrypted confidential information. If remote use of confidential data is required and approved, ITS will provide a secure method of storage.

8. No Deerfield Academy department may store credit card information on any local or networked storage device. Third-party PCI-DSS compliant vendors must be used to process all credit card transactions.

C. *Protection from Disaster or other Unexpected Loss of Data*

1. All electronic data stored on the Academy's network file servers is backed up in a geographically separate location on at least a weekly basis. Backups are retained for a minimum of two weeks. Requests for recovery of data from any backup should be directed to the ITS Help Desk and will require the appropriate approvals.

2. All electronic data systems and services that store or process institutional data are designed and deployed to maximize security, reliability, and availability as follows:

   a. All digital storage is deployed with some form of redundant configuration. This prevents a single device failure from causing data or service loss.

   b. Where possible, ITS deploys servers and services that provide automated failover of the service to another piece of hardware, or migration of the data and service to another piece of hardware, with minimal downtime. This includes: file-server clustering, virtualization of servers, multiple network routes, redundant network devices, and backup/failover servers.

   c. Monitoring tools are used to keep an eye on the status of our production-deployed hardware and services. ITS system administrators are notified automatically of any unexpected outage of a critical resource, to ensure that issues are addressed promptly.

   d. File servers automatically maintain backups of critical files to allow for end-user recovery in the case of accidental overwrite or deletion.

e. The ITS department deploys and manages anti-virus/anti-malware solutions throughout the infrastructure, and on end-user devices. Users may not remove or disable anti-virus/anti-malware tools, and are expected to report suspected malware infections to the ITS Help Desk as soon as they are detected.

D. Data Retention:

a. Business units at Deerfield Academy maintain their own data retention policies and procedures in accordance with best practices and the regulations and laws that are applicable to their business processes.

b. ITS backups of electronic systems provide data retention and recovery beyond the retentions inherent in the data storage technologies themselves. Refer to the *Deerfield Academy Electronic Data Retention Policy* for additional information.

2. The ITS department maintains a disaster recovery plan, which outlines various steps to be taken in the event of a major disaster to maintain the information and communications infrastructures for Deerfield Academy.

E. Additional Policy Documents

1. **Technology Acceptable Use Policy (AUP)**

This policy defines appropriate use of our information systems and networks by students and employees. Violations have the potential to reduce the overall information security posture of the Academy, and to put Confidential information at risk. Non-compliance should be reported immediately to the Director of Information Technology Services, and may have consequences ranging in severity up to and including termination of employment or dismissal from the Academy.

2. **Data Security Incident Response Policy**

This policy defines the proper courses of action to be taken when there is an incident violating any of the policies defined in the WISP, AUP, or any other breach of information security that would expose Deerfield Academy to any risk of financial loss, reputational loss, violation of law, or any other adverse liability. Massachusetts defines a "Data Breach" as *the unauthorized acquisition or unauthorized use of unencrypted data or, encrypted electronic data and the confidential process or key that is capable of compromising the security, confidentiality, or integrity of personal information, maintained by a person or agency that creates a substantial risk of identity theft or fraud against a resident of the Commonwealth*". Any of the above would initiate action according to this Response Policy. Suspicion or evidence of a security breach should be reported immediately to the Director of Information Technology Services or the individual on call for technology emergencies.

F. Miscellaneous

Deerfield Academy provides Information Security and Awareness training to all employees, and provides regular updates in person and via electronic communications.

Any questions or issues regarding information security should be directed to the Director of Information Technology Services.