PRIVACY POLICY

Contents

1 Introduction

Holmwood School takes the safeguarding and handling of data very seriously, this document (and supporting policies) governs the processing of Personal Data, and defines the technical and security measures that must be implemented in order to meet the requirements of the European Union's General Data Protection Regulation (GDPR) and the Data Protection Act 2018, and ensure integrity and availability of the data environment and services.

2 Purpose

Role of Information and Information Systems - Holmwood School is critically dependent on information and information systems. If important information were disclosed to inappropriate persons, the company could suffer serious losses or go out of business. The good reputation that enjoys Holmwood School is also directly linked with the way that it manages both information and information systems. For example, if private customer information were to be publicly disclosed, the Organisation's reputation would be harmed. For these and other important business reasons, executive management working in conjunction with the board of directors has initiated and continues to support an information security effort. One part of that effort is definition of these information security policies.

3 Scope

Involved Persons - Every worker at must comply w Holmwood School ith the information security policies found in this and related information security documents.

Involved Systems - This policy applies to all computer and network systems owned by or administered by this policy. Holmwood School applies to all operating systems, computer sizes, and application systems. The policy covers only information handled by computers and networks. Although this document includes mention of other manifestations of information such as voice and paper, it does not directly address the security of information in these forms.

4 Roles and Responsibilities

Team Effort - To be effective, information security must be a team effort involving the participation and support of every Holmwood School worker who deals with information and information systems. In recognition of the need for teamwork, this policy statement clarifies the responsibilities of users and the steps they must take to help protect Holmwood School information and information systems. This document describes ways to prevent and respond to a variety of threats to information and information systems including unauthorised access, disclosure, duplication, modification, appropriation, destruction, loss, misuse, and denial of use.

Primary Departments Working On Information Security - Guidance, direction, and authority for information security activities are centralized for all Holmwood School Organisational units in the Information Security department [insert an intranet link to the Information Security mission statement]. Information Security is responsible for establishing and maintaining Organisation-wide information security policies, standards, guidelines, and procedures. Compliance checking to ensure that Organisational units are operating in a manner consistent with these requirements is the responsibility of the Information Technology Audit unit within the Internal Audit department [insert a link to the Internal Audit mission statement]. Investigations of system intrusions and other information security incidents are the responsibility of the Physical Security department [insert a intranet link to the Industrial Security mission statement]. Disciplinary matters resulting from violations of information security requirements are handled by local managers working in conjunction with the Human Resources department [insert an intranet link to the Human Resources mission statement].

Three Categories Of Responsibilities - To coordinate a team effort, Holmwood School has established three categories, at least one of which applies to each worker. These categories are Owner, Custodian, and User. These categories define general responsibilities with respect to information security.

Owner Responsibilities - Information Owners are the department managers, members of the top management team, or their delegates within Holmwood School who bear responsibility for the acquisition, development, and maintenance of production applications that process [Organisation] information. Production applications are computer programs that regularly provide reports in support of decision-making and other business activities. All production application system information must have a designated Owner. For each type of information, Owners designate the relevant sensitivity classification, designate the appropriate level of criticality, define which users will be granted access, and approve requests for various ways in which the information will be utilised.

Custodian Responsibilities - Custodians are in physical or logical possession of either [Organisation] information or information that has been entrusted to Holmwood School. While Information Technology department staff members clearly are Custodians, local system administrators are also Custodians. Whenever information is maintained only on a personal computer, the User is also a Custodian. Each type of production application system information must have one or more designated Custodians. Custodians are responsible for safeguarding the information, including implementing access control systems to prevent inappropriate disclosure, and making backups so that critical information will not be lost. Custodians are also required to implement, operate, and maintain the security measures defined by information Owners.

User Responsibilities - Users are responsible for familiarizing themselves with and complying with all Holmwood School policies, procedures, and standards dealing with information security. Questions about the appropriate handling of a specific type of information should be directed to either the Custodian or the Owner of the involved information.

5 Information Classification and Handling

Consistent Information Handling - Holmwood School information, and information that has been entrusted to Holmwood School, must be protected in a manner commensurate with its sensitivity and criticality. Security measures must be employed regardless of the media on which information is stored, the systems that process it, or the methods by which it is moved. Information must be protected in a manner that is consistent with it classification, no matter what its stage in the life cycle from origination to destruction.

Information Classification Designations - Holmwood School has adopted an information classification system that categorizes information into four groupings. All information under Holmwood School control, whether generated internally or externally, falls into one of these categories: Secret, Confidential, Internal Use Only, or Public. All workers must familiarise themselves with the definitions for these categories and the steps that must be taken to protect the information falling into each of these categories. Details can be found in the Information Classification Policy. For purposes of this policy, “sensitive information” is information that falls into either the Secret or Confidential categories.

Information Classification Labelling - If information is sensitive, from the time it is created until the time it is destroyed or declassified, it must be labelled with an appropriate information classification designation. Such markings must appear on all manifestations of the information. The vast majority of Holmwood School information falls into the Internal Use Only category. For this reason, it is not necessary to apply a label to

Internal Use Only information. Information without a label is therefore by default classified as Internal Use Only. Further instructions about labelling sensitive information can be found in the Information Classification Policy.

6 Information Access Control

Need to Know - Access to information in the possession of, or under the control of Holmwood School must be provided based on the need to know. Information must be disclosed only to people who have a legitimate business need for the information. At the same time, workers must not withhold access to information when the Owner of the information instructs that it be shared. To implement the need-to-know concept, Holmwood School has adopted an access request and Owner approval process. Workers must not attempt to access sensitive information unless the relevant Owner has granted them access rights. When a worker changes job duties, including termination, transfer, promotion and leave of absence, his or her supervisor must immediately notify the Information Security department [insert a link with another screen showing details on this notification process]. The privileges granted to all workers must be periodically reviewed by information Owners and Custodians to ensure that only those with a current need to know presently have access.

User IDs And Passwords - To implement the need-to-know process, Holmwood School requires that each worker accessing multi-user information systems have a unique user ID and a private password. These user Ids must be employed to restrict system privileges based on job duties, project responsibilities, and other business activities. Each worker is personally responsible for the usage of his or her user ID and password.

Anonymous User IDs - With the exception of electronic bulletin boards, Internet sites, intranet sites, and other systems where all regular users are intended to be anonymous, users are prohibited from logging into any Holmwood School system or network anonymously. Anonymous access might, for example, involve use of "guest" user IDs. When users employ system commands that permit them to change active user IDs to gain certain privileges, they must have initially logged on employing user IDs that clearly indicated their identities.

Difficult-to-Guess Passwords - Users must choose passwords that are difficult to guess. This means that passwords must not be related to one's job or personal life. For example, a car license plate number, a spouse's name, or fragments of an address must not be used. This also means passwords must not be a word found in the dictionary or some other part of speech. For example, proper names, places, technical terms, and slang must not be used.

Easily Remembered Passwords - Users can choose easily-remembered passwords that are at the same time difficult for unauthorised parties to guess if they:

- string several words together
- shift a word up, down, left, or right one row on the keyboard
- bump characters in a word a certain number of letters up or down the alphabet
- transform a regular word according to a specific method, such as making every other letter a number reflecting its position in the word
- combine punctuation or numbers with a regular word
- create acronyms from words in a song, poem, or another known sequence of words
- deliberately misspell a word
- combine several preferences like hours of sleep desired and favourite colours.

Repeated Password Patterns - Users must not construct passwords with a basic sequence of characters that is then partially changed based on the date or some other predictable factor. Users must not construct passwords that are identical or substantially similar to passwords they have previously employed.

Password Constraints - Passwords must be at least 10 characters long. Passwords must be changed every 90 days or at more frequent intervals. Whenever a worker suspects that a password has become known to another person, that password must immediately be changed.

Password Storage - Passwords must not be stored in readable form in batch files, automatic logon scripts, software macros, terminal function keys, in computers without access control systems, or in other locations where unauthorised persons might discover them. Passwords must not be written down in some readily-decipherable form and left in a place where unauthorised persons might discover them.

Sharing Passwords - If workers need to share computer-resident data, they must use electronic mail, groupware databases, public directories on local area network servers, manual floppy disk exchange, and other mechanisms. Although user IDs are shared for electronic mail and other purposes, passwords must never be shared with or revealed to others. System administrators and other technical information systems staff must never ask a worker to reveal their personal password. The only time when a password should be known by another is when it is issued. These temporary passwords must be changed the first time that the authorised user accesses the system. If a user believes that his or her user ID and password are being used by someone else, the user must immediately notify the system administrator for the information system.

Compliance Statement - All workers who wish to use Holmwood School multi-user computer systems must sign a compliance statement prior to being issued a user ID. Where users already have user IDs, such signatures must be obtained prior to receiving annually-renewed user IDs. A signature on this compliance statement indicates the involved user understands and agrees to adhere to Holmwood School policies and procedures related to computers and networks, including the instructions contained in this policy.

Screenshots – All workers should refrain from taking screenshots that include PII and saving a copy to their desktop or mobile device.

7 Third Party Data Handling

Release Of Information To Third Parties - Unless it has specifically been designated as public, all Holmwood School internal information must be protected from disclosure to third parties. Third parties may be given access to Holmwood School internal information only when a demonstrable need to know exists, when a Holmwood School non-disclosure agreement has been signed, and when such a disclosure has been expressly authorised by the relevant Holmwood School information Owner. If sensitive information is lost, is disclosed to unauthorised parties, or is suspected of being lost or disclosed to unauthorised parties, the information Owner and the Information Security department must be notified immediately.

Third-Party Requests For Holmwood School Information - Unless a worker has been authorised by the information Owner to make public disclosures, all requests for information about Holmwood School and its business must be referred to the Head teacher Such requests include questionnaires, surveys, and newspaper interviews. This policy does not apply to sales and marketing information about Holmwood School products and services, nor does it pertain to customer technical support calls. If a worker is to receive sensitive information from third parties on behalf of Holmwood School this receipt must be preceded by the third-party signature on a Holmwood School release form. For further details on this topic, consult the External Party Information Disclosure Policy. Additional relevant information can be found in the External Communications Security Policy.

External Disclosure Of Security Information - Information about security measures for Holmwood School computer and network systems is confidential and must not be released to people who are not authorised users of the involved systems unless approved by the director of Information Security.

8 Physical Security

Physical Security to Control Information Access - Access to every office, computer machine room, and other Holmwood School work area containing sensitive information must be physically restricted to those people with a need to know. When not in use, sensitive information must always be protected from unauthorised disclosure. When left in an unattended room, sensitive information in paper form must be locked away in appropriate containers. If a Custodian of such information believes he or she will be away for less than 30 minutes, information in paper form may be left on a desk or in some other readily observed spot only if all doors and windows to the unattended room are closed and locked. During non-working hours, workers in areas containing sensitive information must lock-up all information. Unless information is in active use by authorised people, desks must be clear and clean during non-working hours to prevent unauthorised access to information. Workers must position their computer screens such that unauthorised people cannot look over their shoulder and see the sensitive information displayed.

Theft Protection - All Holmwood School's computer and network equipment must be physically secured with anti-theft devices if located in an open office. Local area network servers and other multi-user systems must be placed in locked cabinets, locked closets, or locked computer rooms. Portable computers must be secured with locking cables, placed in locking cabinets, or secured by other locking systems when in an open office environment but not in active use. Computer and network gear may not be removed from [Organisation] offices unless the involved person has obtained a property pass from the building manager. Pagers and cellular phones are not subject to these requirements.

9 Network Security

Internal Network Connections - All Holmwood School's computers that store sensitive information, and that are permanently or intermittently connected to internal computer networks must have a password-based access control system approved by the Information Security department. Regardless of the network connections, all stand-alone computers handling sensitive information must also employ an approved password-based access control system [insert a link to approved information security products list and procurement details on how to order them]. Users working with all other types of computers must employ the screen saver passwords that are provided with operating systems, so that after a period of no activity the screen will go blank until the correct password is again entered. Multi-user systems throughout [Organisation] must employ automatic log off systems that automatically terminate a user's session after a defined period of inactivity.

External Network Connections - All in-bound session connections to [Organisation] computers from external networks must be protected with an approved dynamic password access control system [insert a link to approved information security products list]. Dynamic passwords are different each time they are used, and therefore cannot be replayed to gain unauthorised access. Users with personal computers connected to external networks are prohibited from leaving unattended modems turned-on while data communications software is enabled, unless an authorised dynamic password system has been previously installed. When using [Organisation] computers, [Organisation] workers must not establish connections with external networks including Internet service providers unless these connections have been approved by the Information Security department. For further information on this process, see the External Communications Security Policy [insert a link].

Network Changes - With the exception of emergency situations, all changes to [Organisation] computer networks must be documented in a work order request, and approved in advance by the Information Technology department. All emergency changes to [Organisation] networks must be made only by persons who are authorised by the Information Technology department. This process prevents unexpected changes from inadvertently leading to denial of service, unauthorised disclosure of information, and other problems. This process applies not only to workers but also to vendor personnel.

Telecommuting - At management's discretion, certain qualified workers can do some of their work at home. Permission to telecommute must be granted by each worker's immediate supervisor based on a checklist of relevant factors [insert link to the checklist, which may be a subsidiary intranet page under the Human Resources department's main intranet page]. Continued permission to telecommute is partially dependent on continued compliance with a number of information security policies and standards. For further information on these requirements, see the Telecommuting Policy [insert a link]. Periodic checking of electronic mail while on the road or from home is not considered telecommuting, but does require that workers follow many of the same security precautions.

10 Internet and Electronic Mail

Internet Access - Workers are provided with Internet access to perform their job duties, but this access may be terminated at any time at the discretion of a worker's supervisor. Internet access is monitored to ensure that workers are not visiting sites unrelated to their jobs, and also to ensure that they continue to be in compliance with security policies. Workers must take special care to ensure that they do not represent [Organisation] on Internet discussion groups and in other public forums, unless they have previously received top management authorization to act in this capacity. All information received from the Internet should be considered to be suspect until confirmed by reliable sources. Workers must not place [Organisation] material on any publicly-accessible computer system such as the Internet unless the posting has been approved by both the information Owner and the director of the Information Technology department. The establishment of Internet pages is separately handled by an approval process involving the external communications committee [insert a link to the Public Relations department]. Users are prohibited from establishing any electronic commerce arrangements over the Internet unless Information Technology and the Information Security department have evaluated and approved of such arrangements. Sensitive information, including passwords and credit card numbers, must not be sent across the Internet unless this information is in encrypted form. These and related considerations are discussed in greater detail in the Internet Communications Policy.

Electronic Mail - Every [Organisation] worker who uses computers in the course of their regular job duties will be granted an Internet electronic mail address and related privileges. All [Organisation] business communications sent by electronic mail must be sent and received using this company electronic mail address. A personal Internet service provider electronic mail account or any other electronic mail address must not be used for [Organisation] business unless a worker obtains management approval. When transmitting messages to groups of people outside [Organisation], workers must always use either the blind carbon copy facility or the distribution list facility. Unsolicited electronic mail transmissions to prospects and customers are prohibited. Emotional outbursts sent through electronic mail and overloading the electronic mail account of someone through a deluge of messages are forbidden. All business electronic mail communications must be proofread before they are sent, and professional and business like in both tone and appearance. Electronic mail is a public communication method much like a postcard. All [Organisation] workers must refrain from sending credit card numbers, passwords, or other sensitive information that might be intercepted. All [Organisation] staff must additionally employ a standard electronic mail signature that includes their full name, job title, business address, and business telephone number. Users should not store important messages in their electronic mail inbox. Additional details can be found in the Electronic Mail Security Policy.

Computer Virus Screening - All personal computer users must keep the current versions of approved virus screening software enabled on their computers [insert a link to list of approved information security products]. Users must not abort automatic software processes that update virus signatures. Virus screening software must be used to scan all software and data files coming from either third parties or other [Organisation] groups. This scanning must take place before new data files are opened and before new software is executed. Workers must not bypass or turn off the scanning processes that could prevent the transmission of computer viruses.

Computer Virus Eradication - If workers suspect infection by a computer virus, they must immediately stop using the involved computer and call the help desk [insert a link to the help desk page]. Floppy disks and other magnetic storage media used with the infected computer must not be used with any other computer until the virus has been successfully eradicated. The infected computer must also be immediately isolated from internal networks. Users must not attempt to eradicate viruses themselves. Qualified [Organisation] staff or consultants must complete this task in a manner that minimizes both data destruction and system downtime.

Clean Backups - All personal computer software must be copied prior to its initial usage, and such copies must be stored in a secure location such as a locked file cabinet. These master copies must not be used for ordinary business activities, but must be reserved for recovery from computer virus infections, hard disk crashes, and other computer problems.

Software Sources - [Organisation] computers and networks must not run software that comes from sources other than other [Organisation] departments, knowledgeable and trusted user groups, well-known systems security authorities, or established computer, network, or commercial software vendors. Software downloaded from electronic bulletin boards, shareware, public domain software, and other software from untrusted sources must not be used unless it has been subjected to a rigorous testing regimen approved by the Information Security department [insert a link to a page describing this process and who to contact].

Written Specifications for Owners - All software developed by in-house staff, intended to process critical or sensitive [Organisation] information, must have a formal written specification. This specification must include discussion of security risks and controls including access control systems and contingency plans. The specification must be part of an agreement between the information Owner and the system developer. Macros in spreadsheets and word processing documents are not considered software in this paragraph.

Security Sign-Off Required - Before being used for production processing, new or substantially changed application systems must have received written approval from the

Information Security department for the controls to be employed. This requirement applies to personal computers just as it does to larger systems [insert a link to form requesting Information Security department review and sign-off].

Formal Change Control - All computer and communications systems used for production processing must employ a documented change control process that is used to ensure that only authorised changes are made. This change control procedure must be used for all significant changes to production system software, hardware, communications links, and procedures. This policy applies to personal computers running production systems and larger multi-user systems. For further information on this topic, see the Software Development And Change Control Policy [insert a link].

Systems Development Conventions - All production software development and software maintenance activities performed by in-house staff must adhere to Information Technology department policies, standards, procedures, and other systems development conventions. These conventions include the proper testing, training, and documentation. For further information on this topic, see the Software Development And Change Control Policy.

Adequate Licenses - [Organisation] management must make appropriate arrangements with software vendors for additional licensed copies, if and when additional copies are needed for business activities. All software must be purchased through the Procurement department.

Unauthorised Copying - Users must not copy software provided by [Organisation] to any storage media, transfer such software to another computer, or disclose such software to outside parties without advance permission from their supervisor. Ordinary backup copies are an authorised exception to this policy.

Backup Responsibility - Personal computer users must regularly back up the information on their personal computers, or ensure that someone else is doing this for them. For multi-user computer and communication systems, a system administrator is responsible for making periodic backups. If requested, the Information Technology department must install, or provide technical assistance for the installation of backup hardware and software. All backups containing critical or sensitive information must be stored at an approved off-site location with either physical access controls or encryption. A contingency plan must be prepared for all applications that handle critical production information. It is the responsibility of the information Owner to ensure that this plan is adequately developed, regularly updated, and periodically tested.

11 User Rights and Expectations

Rights To Material Developed - While performing services for Holmwood School workers must grant to Holmwood School exclusive rights to patents, copyrights, inventions, or other intellectual property they originate or develop. All programs and documentation generated by, or provided by workers for the benefit of Holmwood School are the property of Holmwood School. Holmwood School asserts the legal ownership of the contents of all information systems under its control. Holmwood School reserves the right to access and use this information at its discretion.

Right To Search And Monitor Holmwood School management reserves the right to monitor, inspect, or search at any time all [Organisation] information systems. This examination may take place with or without the consent, presence, or knowledge the involved workers. The information systems subject to such examination include, but are not limited to, electronic mail system files, personal computer hard drive files, voice mail files, printer spool files, fax machine output, desk drawers, and storage areas. All searches of this nature must be conducted after the approval of the Legal and Security departments has been obtained. Because Holmwood School computers and networks are provided for business purposes only, workers must have no expectation of privacy associated with the information they store in or send through these information systems. Holmwood School management retains the right to remove from its information systems any material it views as offensive or potentially illegal.

Personal Use - Holmwood School information systems are intended to be used for business purposes only. Incidental personal use is permissible if the use does not consume more than a trivial amount of resources that could otherwise be used for business purposes, does not interfere with worker productivity, and does not pre-empt any business activity. Personal use that does not fall into these three categories requires the advance permission of a department manager. Use of Holmwood School information systems for chain letters, charitable solicitations, political campaign material, religious work, transmission of objectionable material, or any other non-business use is prohibited.

Unbecoming Conduct - Holmwood School management reserves the right to revoke the system privileges of any user at any time. Conduct that interferes with the normal and proper operation of Holmwood School information systems, which adversely affects the ability of others to use these information systems, or that is harmful or offensive to others is not permitted.

Security Compromise Tools - Unless specifically authorised by the Information Security department, Holmwood School workers must not acquire, possess, trade, or use hardware or software tools that could be employed to evaluate or compromise information systems security. Examples of such tools include those that defeat software copy protection, discover secret passwords, identify security vulnerabilities, or decrypt encrypted files. Without this type of approval, workers are prohibited from using any hardware or software that monitors the traffic on a network or the activity on a computer.

Prohibited Activities - Users must not test, or attempt to compromise computer or communication system security measures unless specifically approved in advance and in writing by the director of the Internal Audit department. Incidents involving unapproved system hacking, password guessing, file decryption, bootleg software copying, or similar unauthorised attempts to compromise security measures may be unlawful, and will be considered serious violations of [Organisation] internal policy. Short-cuts bypassing systems security measures, and pranks and practical jokes involving the compromise of systems security measures are absolutely prohibited.

Mandatory Reporting - All suspected policy violations, system intrusions, virus infestations, and other conditions that might jeopardize Holmwood School information or Holmwood School information systems must be immediately reported to Head Teacher.

The Information Security manager acknowledges that under rare circumstances, certain workers will need to employ systems that are not compliant with these policies. All such instances must be approved in writing and in advance by the Information Security manager.

12 Violations

Any violation of this policy may result in disciplinary action, up to and including termination of employment. Holmwood School reserves the right to notify the appropriate law enforcement authorities of any unlawful activity and to cooperate in any investigation of such activity. Holmwood School does not consider conduct in violation of this policy to be within an employee's or partner's course and scope of employment, or the direct consequence of the discharge of the employee's or partner's duties. Accordingly, to the extent permitted by law, Holmwood School reserves the right not to defend or pay any damages awarded against employees or partners that result from violation of this policy.