Policy: Data & Information Security

Review: **May 2020**
Approved: **10th May 2018 (Resources)**
Approved: **16th May 2016 (FGB)**

Contents:

Introduction

1.1 This policy explains Sidmouth College's expectations regarding the use of computer equipment and access to information. It is intended to protect all systems and information assets owned and used by Sidmouth College from the risks posed by inappropriate use, including unauthorised or unlawful access, accidental or deliberate loss, damage, theft, disclosure or destruction.

1.2 All information entrusted to the College must be managed, stored and processed lawfully and appropriately within the requirements of legislation including "The Data Protection Act 1998", "Freedom of Information Act 2000", "Computer Misuse Act 1990", "The Human Rights Act 1998" and "General Data Protection Regulation 2018". The data protection principles in the "Data Protection Act" state that organisations are **required** take technical and organisational measures to prevent "unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data." The College maintains the confidentiality of personal information held on its computers and manual records.

1.3 It is the personal responsibility of **all** employees or other persons having access to the College's systems and information to comply with this policy and keep equipment and information secure. Agency workers and sub-contractors who are required to use College systems should also be made aware of, and will be expected to comply with, this policy.

1.4 Any deliberate breach of this policy could amount to a criminal offence. All incidents will be investigated and may result in formal disciplinary procedure. A serious breach of this policy could be regarded as gross misconduct and may lead to dismissal and / or criminal action being taken.

1.5 As well as statutory requirements, Sidmouth College recognises the need to comply with best practice in securely managing the information in its care to avoid:

- causing any loss of data which might cause extreme embarrassment, put individuals at risk and affect personal, professional or organisational reputation.
- to avoid the criticism and negative publicity that could be generated by any loss of personal data.

1.6 It is the responsibility of **all** members of the College community to ensure that when handling, using or transferring data, the following principles are followed:

- Data confidentiality – only authorised persons should have access to data.
- Data integrity – all authorised users should feel confident that data about them is accurate and not improperly modified
- Data availability – authorised users should be able to access the data they need, when they need it.
- Asset security – the school's physical network assets should be protected and made available for use by authorised users only.

Scope

2.1 To comply with statutory requirements and principles of best practice, this policy refers to all forms of personal data regardless of whether it is held on paper or in electronic format and from wherever that data is accessed within or remote from the school site.

2.2 The Data Protection Act 1998 defines **'personal data'** as data which relate to a living individual who can be identified, and includes any expression of opinion about the individual or reference to them. It's impossible to specify **every** item of data covered by the Act but would include the following;

- Personal information about staff, students, parents, carers such as names, addresses, contact details, health records, disciplinary records
- Class lists, progress records, reports, references
- Staff employment history, taxation, National Insurance records, appraisal records and references,
- Any information disclosed by parents, carers or agencies working with families or staff.

Roles & Responsibilities

3.1 The Senior Information Risk Owner (SIRO) is a senior member of staff who is ultimately responsible for all matters relating to information security and is also responsible for appointing the Information Asset Owners (see below) and ensuring a risk assessment is conducted.

The Sidmouth College SIRO are the Co-Principals.

3.2 Information Asset Owner (IAO) should identify information assets within their area of responsibility including any personal data such as assessment records, medical information and special educational needs data. Information assets also include non-personal data that could be considered sensitive if lost or corrupted, such as financial data, commercial data, organisational and operational data, and correspondence.

3.3 The IAO's role is to understand and manage

- what information is held and for what purposes,
- who has access to the data and why
- how the data will be amended or added to if necessary
- how information is retained and disposed off

3.4 It is the responsibility of the Principal to ensure compliance with this policy. All systems within the College containing information about individuals must be identified and made secure. It is the responsibility of all employees to co-operate in this task. Upon discovering that the College's Policy on Data Protection is not being complied with the Principal, after consultation with the County Solicitor, shall have full authority to take such immediate steps as considered necessary.

3.5 Sidmouth College will ensure that personal information is processed in accordance with an individual's rights. It will provide to any individual who requests it in the proper manner, a reply stating whether or not the College holds computer personal information about that individual and, if so, a written copy in clear language of the current information held, its purposes, the source of the information and people to whom it is disclosed. The College shall fix a fee for this service which in appropriate circumstances may be waived by the Principal in consultation with the County Treasurer.

Access & Permissions

4.1 It is the responsibility of all members of the school community to ensure that access to Sidmouth College's school infrastructure and network is as safe and secure as is reasonably possible. Everyone needs to take care when handling, using or transferring personal data so that it cannot be accessed by unauthorised person. In particular,

- users must only access or attempt to access systems or data for which they have authorisation
- users must not access or attempt to access any other person's files or information without permission.
- users must take reasonable steps to ensure information in their care is held securely at all times.

4.2 The College will ensure that user access is controlled and monitored through:

- use of unique user-ids with the correct confidential password before access is allowed to College systems.
- appropriately logging user access and activity whilst using College systems

4.3 Sidmouth College expects all of the college employees, or anyone providing a service to the College, to comply fully with this policy and the Data Protection Act principles. They must make sure the information is:

- used fairly and lawfully
- used for limited, specifically stated purposes
- used in a way that is adequate, relevant and not excessive
- accurate
- kept for no longer than is absolutely necessary
- handled according to people's data protection rights
- kept safe and secure
- not transferred outside the UK without adequate protection

4.4 Sidmouth College will hold the minimum personal information necessary to enable it to perform its functions, and the information will be erased once the need to hold it has passed. Every effort will be made to ensure that information is accurate, up-to-date and that inaccuracies are corrected without unnecessary delay. Care will be taken to ensure that information about an individual is not transferred to countries outside the European Economic Area without the individual's consent or someone acting on their behalf. An example of overseas transfer would be the publishing of information on the Internet.

4.5 Personal information is confidential. Information systems will be designed to comply with the Data Protection principles. Personal information will be disclosed only for registered purposes to:

- College staff where such information is vital to their work.
- Others as detailed in the Registration.
- The Courts under the direction of a Court Order.
- Under limited exemptions that allow for disclosures e.g. those required by law or for the prevention and detection of crime or apprehension and prosecution of offenders.

Passwords

5.1 Access to all Sidmouth College systems will be via secure user IDs and passwords and will be controlled by the Network Manager. Groups of users will have clearly defined access rights depending on their needs. Full, secure records will be kept of user IDs, user log-ons and security incidents. The IT team may check compliance with these requirements at any time.

5.2 The "administrator" access rights for the school ICT system, used by the Network Manager (or other person) must also be available to a nominated senior leader and kept in a secure place (e.g. school safe).

5.3 All Sidmouth College staff or any other authorised user of Sidmouth College IT systems must ensure that passwords:

- should be hard to guess but easy to remember
- should not be written down, or kept where others might find them.
- must never be shared or revealed to anyone under any circumstances.
- must contain at least eight characters including a mixture of upper and lower case letters, numbers and special characters such as ! # £ $.
- should be changed the next time users login after initial set up or after a password reset
- are changed regularly or when prompted by the system.
- are changed immediately if it is suspected or known to have been compromised. Such incidents must be reported to the appropriate Information Risk Officer (in this case, the Network Manager).
- must not be stored in readable form in batch files, automatic logon scripts, software macros, in computers without access control or in other locations where unauthorised persons might discover or use them.
- must not be stored in an internet browser or data communications software at any time. The "Remember Password" feature should not be used when accessing any College systems.

5.4 Any suspected violation of this policy may be investigated by the Senior Information Risk Officer (Principal) and may lead to disciplinary action.

Physical Security

6.1 Care must be exercised with the physical security of computer equipment or media to ensure that there is no accidental loss, damage or unavailability of data (also applies when working from home).

6.2 Computer equipment must not be positioned where it is at risk from being knocked over or having liquids spilt on it.

6.3 Only approved cleaning products should be used; never spray water or foam based cleaners directly onto computer equipment

6.4 Desktop computing equipment should never be moved to a different location in the office without prior arrangement with the IT team.

6.5 Any portable devices left unattended must be password protected and secured against theft by devices such as Kensington locks

6.6 Password protected screensavers should be employed when leaving display screens unattended

6.7 Sidmouth College computing equipment may only be taken off premises with prior approval of the Network Manager.

Acceptable Usage

7.1 All Sidmouth College computing resources are supplied to aid teaching and learning. Failure to observe secure working practices could lead to compromise or corruption of data, or malfunction or unavailability of the system.

7.2 Users are not permitted to install unauthorised software and should not customise or make copies of software unless it is an established part of their job. Examples of unauthorised software include but are not limited to:

- games
- unlicensed or pirated software
- public domain software and shareware (e.g. software downloaded from the Internet or from magazine cover disks)
- any software obtained privately
- Any requirements for additional software must be forwarded to the IT team.

7.3 The following rules must be adhered to.

- Everyone must read and agree to comply with the Sidmouth College security policies before using any College computing resource
- Users must not share their account with anyone else.
- Users must not use a computer that someone else has logged into unless you are authorised to do so as part of their job.
- Contracted staff will only be allocated user-ids for specific purposes, e.g. a contracted computer engineer, and this must be authorised by the Network Manager, based on an assessment of the risk involved.
- Each user will only be provided with access to relevant material necessary for their day-to-day responsibilities and for which they have been trained and authorised, including general material that is required by all users.
- You must only connect Sidmouth College supplied and authorised equipment to any Sidmouth College computers or networks. Any equipment outside of the normal scope, needs to be referred to the Network Manager.

- You should not reconfigure any hardware, software, network, or any other type of device, unless you are authorised to do so as part of your job. You must address any configuration change requirements to your IT team stating the business need.
- You must never remove the cover from any computer equipment, unless you are authorised to do so as part of your job.
- All work files must be stored in directories on the network servers (Such as the H: drive).
- You MUST lock your computer when leaving it unattended.
- A password protected screen saver will be activated after 30 minutes of inactivity.
- All unexpected or suspicious warning messages must be reported to your IT team. Also, if you have any reason to suspect your PC has a virus, you must stop work immediately and tell your IT team. This is important even if the message states that a virus has been successfully removed, because the PC may still attempt to infect others.
- You must not attempt to fix problems with your computer, whether hardware, software or network related, unless you are authorised to do so as part of your job. All problems must be reported to your IT team immediately, unless you know it is already under investigation.
- At the end of each working day you must log off your PC and turn it off.
- You may be held personally liable for any misuse of Sidmouth College computing resources or for any other breach of this policy.

Personal Use

8.1 Sidmouth College supplied computing resources are provided for official use, however Sidmouth College will permit occasional and reasonable personal use in an individual’s own time to enter, access, store or reproduce data that is not work related, but this activity must not:

- break the law;
- risk bringing Sidmouth College into disrepute or placing it in a position of liability;
- cause damage or disruption to Sidmouth College systems;
- use unreasonable amounts of official time, or interfere with official duties;
- add significantly to our running costs;
- otherwise infringe this Data Security Policy, the Email Usage Policy, the Internet Usage Policy or any of the usual standards of personal conduct which apply in Sidmouth College, as set out in the Staff Handbook

8.2 Limited use of the College's internet and email systems is allowed for private use provided:

- Employees comply with the College's published E-mail and Internet policies.
- It is not in the College's time.
- It does not interfere with the employees work or that of colleagues.
- It does not incur the College additional cost (such as subscription to email mailing lists).
- It does not put an extra burden on the network and it affects its performance.
- It is evident to others that the use is personal and there is no risk that the name of the College is inadvertently brought into disrepute.

8.3 The following activities are **expressly forbidden**

- Conducting any activity that may be considered offensive by other staff, such as the creating or processing of any racist, sexist, obscene or defamatory material;
- Running a commercial business, such as selling and advertising;
- Any hacking activity

You must consult your line manager if you have any doubts as to what is reasonable use.

Portable Computers and Removable Storage Media

9.1 The preferred means of accessing personal or sensitive data outside of the school site is by using FOLDR, providing a secure connection to the College Systems. When this is not possible, portable computers or encrypted removable storage media provided by Sidmouth College may be used.

9.2 To prevent unauthorised or unlawful access, loss, damage, theft, or disclosure of information users must ensure that all mobile devices and storage media containing personal or sensitive data are encrypted using approved encryption software, password protected (including screensavers) and transported and stored securely. Users must take particular care that such devices must not be accessed by other unauthorised users (e.g. family members) when out of school. Unencrypted memory sticks must not be used on the College system by staff. All staff issued laptops must be fully encrypted.

9.3 All media must be used and stored in line with the manufacturer's instructions and held securely when not in use. Data that is no longer required on media should be securely erased.

9.4 Personal or sensitive data can only be passed to external organisations with the authorisation of the Senior Information Risk Officer. New or securely erased media should be used and care must be taken that only the data that is being exported has been copied to the media and that no other data is on it.

9.5 When using laptops and removable media, the computer's antivirus software must be active and its virus definition file must be up to date.

9.6 If there is any reason to believe that passwords or physical security has been compromised, contact the IT department immediately.

Incident Handling

10.1 An information security incident relating to a breach or suspected breach of confidentiality could be anything from computer users sharing passwords to a piece of paper identifying an individual being found in a public area. All breaches of security and/or confidentiality could compromise business operations, result in embarrassment or loss of trust in Sidmouth College. These breaches could be a threat to the personal safety or privacy of an individual(s) and/or lead to legal or penalty issues. Examples of these types of incident include:

- damage to or theft/loss of information (either manual or electronic)
- the finding of confidential information/records in a public area
- poor disposal of confidential waste
- unauthorised access to information
- unauthorised disclosure of confidential information to a third party (in any format including verbally)
- transfer of information to the wrong person (by email, fax, post, or phone)
- receiving of information (such as by email or fax) meant for someone else

- sharing of computer IDs and passwords.

Every breach must be taken seriously and reported to the IT team

10.2 After taking appropriate action, The Network Manager will consider whether the matter should be reported to Devon County Council’s Information Governance Team.

10.3 All incidents relating to breaches of security and confidentiality, where there has been a theft/loss of IT equipment, must also be reported to the IT team. If necessary, this should also be reported to Devon County Council’s Information Governance Team.

Disposal of Equipment

11.1 Sidmouth College is responsible for ensuring that no personal, confidential or sensitive information remains on any redundant equipment or media which is intended for disposal or recycling. The College contracts a third party to provide secure disposal of equipment. All equipment, whether for disposal or internal recycling must be returned to the IT department. Recycled equipment must have all data securely erased before being redeployed.