Sutton Valence Senior School

svs.org.uk

Information Security Policy

The School is committed to using information technology and computer systems in a secure, efficient and legitimate manner. It fully supports compliance with GDPR, and other legislation relating to the use of computers.

Introduction
It is essential that all information processing systems within the School are protected to an adequate level from disruption and loss of service, whether through accident or deliberate damage.

The document outlines the School's policy in relation to the use of computers and especially the areas of:

- Fraud;
- Theft;
- Use of unlicensed software;
- Private work;
- Hacking;
- Sabotage;
- Misuse of personal data;
- Use of the internet and email;
- Disposal of equipment.

Purpose of the Security Policy
The purpose of the policy is to provide a set of rules, measures and procedures that determine the School's commitment to ensuring that its IT (Information Technology) resources are protected from physical and logical risk.

The main objectives of the policy are:

- To ensure that all the School's assets, staff, students, data and equipment are adequately protected against any action that could adversely affect the IT services required to conduct the School's business;
- To ensure that staff and students are aware and comply with all relevant legislation and School policies related to how they conduct their day-to-day duties in relation to IT.

Application of the Security Policy
The policy is relevant to all IT services, irrespective of the equipment in use, or location, and applies to:

- All staff and students;
- Employees and agents of other organisations who directly or indirectly support or use the School's Computer Services;
- All use of IT services within the School.

Management of the IT Policy
IT security is the responsibility of the staff, students, Network Manager and Director of ICT.

The policy has been reviewed in terms of the policy's scope, content and effectiveness.

The School role of Information Security Officer will be part of the remit of the Director of ICT whose responsibilities will include implementing, monitoring, documenting and communicating information security in compliance with the security policy and legislation. The current Director of ICT is Glen Millbery.

The Director of ICT is responsible for ensuring that all staff are aware of their responsibilities under the policy and have access to the contents of this document.

All providers of IT services must ensure the security, integrity and availability of data within the service provided.

The IT policy document is intended to be a living document, which will be updated, as and when necessary. Sections and appendices can be added to reflect new or amended procedures and guidelines when determined.

Violations
Violations of this policy may include, but are not limited to, any act that:

- Exposes the School to actual or potential monetary loss through the compromise of IT security;
- Involves the disclosure of confidential information or the unauthorised use of corporate data;
- Involves the use of data, which causes, for example, the law to be broken.

Any individual who suspects that this policy is being violated by another individual must report the violation immediately to the Network Manager or Director of ICT.

A log of all security incidents will be kept by the Director of ICT. The log records any reported incidents and action taken.

Any breach of the security policy will be investigated and may result in the individual being subjected to the School's disciplinary procedure.

Legislation Compliance
The School has to comply with all UK legislation affecting IT. All organisations, employees, staff and students must comply with the following Acts.

The following are brief descriptions on key legislation affecting IT users.

General Data Protection Regulation (GDPR) 2018

- Computers are in use throughout society – collating, storing, processing and distributing information. Much of the information is about people - personal data. This is subject to the GDPR;
- The School is only allowed to record and use personal data if there is a legitimate purpose for doing so and if details of the information, its use and source have been registered with the Data Commissioner. There are strict rules about how the information is used and to whom it is disclosed;
- The GDPR gives rights to individuals about whom information is recorded on computer and in certain manual files. They may request copies of the information about themselves challenge it if appropriate and claim compensation in certain circumstances;
- If there is any doubt about whether the information can be collected, used or disclosed please address queries to the School's designated Data Compliance Officer – Glen Millbery.

Copyright Designs and Patent Act 1998

- Under this Act, any duplication of licensed software or associated documentation (e.g. manuals) without copyright owner's permission is an infringement under copyright law. All proprietary software manuals are usually supplied under licence agreement, which limits the use of the products to specified machines and will limit copying to the creation of backup copies only. However in some instances, site licenses, permitting the use of software on all machines within a specified site are obtainable;
- To combat the problems of illegal copying, software suppliers have formed their own organisation to police the use of software throughout the UK. The 'Federation Against Software Theft' (FAST) is able to conduct spot checks on organisations, including local authorities, under a court order and without prior warning;
- According to the Act, individuals found to be involved in the illegal reproduction of software may be subject to unlimited civil damages and to criminal penalties including fines and imprisonment.

Computer Misuse Act, 1990

- The Computer Misuse Act, 1990 was introduced to deal with three specific offences that were not adequately covered under existing laws:
    - Unauthorised access or attempt to access computer material (such as 'hacking'). Under this offence it is not necessary to prove the users intent to cause harm;
    - Unauthorised access with intent. For example, hacking is carried out with the intention of committing a more serious crime such as fraud. Under this offence, if a plan has been hatched which involves the unauthorised use of a computer, the unauthorised use will be sufficient to prove an attempt to commit the crime;
    - Unauthorised modification. This part of the act makes it an offence to intentionally cause unauthorised modification such as the introduction of viruses;
- The intention of the act is to enable an organisation to take legal action to protect their data and equipment from unauthorised access and damage.

Health and Safety Act (1992)

- The School shall ensure, through the appointed Health and Safety Officer that all IT equipment is located and used in such a way to not impede health of users or others.

Defamation

- Facts concerning individuals or organisations must be accurate and verifiable. Views or opinions must not portray their subjects in any way, which could damage their reputation.

Race Relations Act (1976) and Sex Discriminations Act (1976)

- Accessing or distributing material, which might cause offence to individuals or damage the School's reputation, is forbidden. For example pornographic, racist or sexist material.

Criminal Justice and Public Order Act 1994 and Obscene Publications Act (1959 & 1964)

- To ensure this law is complied with, any use of the School's computer equipment for viewing, reading, downloading, uploading, distributing, circulating or selling any material which is pornographic, obscene, racist, sexist, grossly offensive or violent is strictly forbidden. This is irrespective of laws regarding the material in the country of origin.

Human Rights Act 1998 (operative October 2000)

- Under this Act, everyone has a right to respect for their private life, their home and correspondence, which is commensurate with the need to protect the School from fraud, introduction of viruses or breach of other overriding considerations. To this end, the School reserves the right to monitor usage of PC's and telephones;
- There is a separate policy on the monitoring of electronic communications;
- Individuals using the internet, email or telephone should respect the confidence of the School and colleague's information in disclosing it to other people. Email, in particular, should not be circulated in a tone, which may give rise to a claim of inhuman or degrading treatments.

Regulatory Investigatory Powers (RIP) Act 2000

- Interception of communications including computer communications such as email, are unlawful unless in accordance with the RIP Act 2000;
- The School may monitor and record communications for the following purposes:-
- To establish facts and monitor performance of standards;
- In the interests of national security;
- To deter crime;
- To detect unauthorised use of the system;
- To secure a system.

The policy for the Use of Electronic Communications details how the RIP Act is implemented within the School.

Assets Classification and Control

The School positively identifies and keeps documentary evidence of all computer equipment.

It is the responsibility of the Network Manager and Director of ICT to ensure that these records are accurate and continuously maintained.

The inventory is maintained using a database, including information relating to location and asset tag number/serial number.

On receipt of new equipment it must be labelled and recorded on the inventory. No IT equipment should be purchased without prior consultation with the Network Manager or Director of ICT.

No equipment should be installed on the School's network without prior consent of the Network Manager who must first record the equipment within the inventory.

All disposals of equipment should be recorded against its original entry.

No equipment should be relocated without prior consultation with the Network Manager.

Personnel Security

All staff commencing employment with the School agree to comply with this policy and its associated policy for the Use of Electronic Communications.

Personnel procedures ensure that all Staff are made aware of these policies during their induction process.

Copies of all the policy and guidance notes are available from via the School's network.

Training
Each new employee is made aware of his or her obligations for security during the School's induction-training program. This includes staff being told of the existence of the policies and where to find them.

Training requirements are reviewed on a regular basis to take account of the needs of the individual, and to ensure that staff are adequately trained in the use of technology.

Where training is required for a specific application this may be carried out in consultation with the Network Manager and Director of ICT.

Physical Security
Physical Access Controls
The Director of ICT has a responsibility for ensuring that staff leaving the School's employment account for their computer equipment, including software and related manuals and peripherals.

Access to the computer rooms is clearly defined as a security perimeter. Access is controlled by a locked door. Unless a member of staff is present within the room the door should be locked and no students present.

Security of Equipment
Where possible computer equipment is sited away from public areas. Where this is not possible the equipment is always supervised.

Computer screens and printed output should not be in view of unauthorised persons.

All computer screens that are in public areas should be controlled by time delayed screensavers which require a password to access information.

Staff should take responsibility for the physical security of their computer equipment within their working environment. Windows and doors should be kept shut whilst unattended.

Power Supplies
Critical equipment is protected from potential power loss by uninterruptable power supplies (UPS).

All UPSs are periodically tested and upgraded where necessary.

Cable Security
All networking devices (i.e. routers) are securely located within School premises. Power and telephone lines into the computer suite are underground where possible.

Equipment Maintenance
All equipment is maintained to ensure availability. Critical systems are supported by annual maintenance agreements, which provide for technical support and call out.

IT equipment is maintained by the Network Manager. Repairs and servicing should only be carried out by authorised staff and contractors.

Staff who wish to report faults of their equipment are able to do so by telephoning or emailing ICT Support.

Security of Equipment off-premises
Portable computers are very vulnerable to theft; loss and unauthorised access when travelling. Personnel who have portable equipment should familiarise themselves with the instructions included in the Laptop Policy.

The high incidence of car theft makes it inadvisable to leave equipment or media in an unattended vehicle.

All portable computer equipment is insured with the School's insurance, except when left unattended in a vehicle.

All USB devices that are plugged into School-owned laptops will automatically be encrypted with BitLocker encryption.

Computer Management
Operational procedures
All regular operational procedures are fully documented and have restricted access to authorised personnel.

Backup and system procedures are kept of all fundamental systems, including:

- General operations of computer services;
- Day-to-day operations and work schedules;
- Month-end and year-end procedures;
- Recovery procedures.

Incident Management Procedures
All system failures are logged and recorded by the Network Manager. The Network Manager is responsible for investigating, resolving the failure, and implementation of remedies to prevent reoccurrence.

Segregation of Duties
Segregation of duties are in place wherever practically possible. The objective is to minimise the risk of negligent or deliberate misuse of computer systems.

Capacity Planning
The Network capacity is monitored to ensure that there are adequate system resources. These include processors, main storage, file storage, printers and other output devices.

Protection from Malicious Software
The School uses antivirus software as a means of protecting itself from malicious attack.

All servers and workstations are installed with up-to-date antivirus software.

The Network Manager periodically checks to ensure that all workstations and servers are updated with the most up-to-date version of antivirus software available.

Staff are instructed to report all virus incidents, including hoaxes, immediately to ICT Support.

The Network Manager may notify staff periodically of any relevant procedures for specific virus prevention.

Housekeeping
The Network Manager regular reviews data stored on the network to ensure that it continues to conform to operational requirements and the requirements of the GDPR. Surplus data is archived or removed after consultation with the relevant parties.

Data Backup/Media Storage
Back-up copies are taken of all essential data, software and system files daily. The backup procedures ensure that all critical systems can be recovered in the event of a disaster.
Backups are checked daily to ensure that they have completed. Records of all backups are kept securely.

Backup procedures are tested regularly. Records are maintained of all successful restores.

Network Management
Network Security Controls
The Director of ICT and the Network Manager have the responsibility for the security of data on the network and protect connected services from unauthorised access.

The Network Manager has responsibility for security access to the network.

Network Access
Network access is controlled by the Network Manager.

Users and their access to resources are created, modified and deleted as appropriate when requested. No access or amendment is made unless appropriate authorisation is received from the data owner.

Access by third parties (software maintenance) to the network is only allowed in the following circumstances:

- The Network Manager has confirmed in advance that maintenance is due to take place;
- The identity of the user is known to the Manager;
- The Network Manager is present whilst work is being undertaken.

Security of System Documentation
All systems should be adequately documented. Documentation is kept up-to-date and matches the state of the system at all times.

Systems documentation is physically secured at all times with access restricted to authorised personnel. An additional copy should be kept (hardcopy or softcopy), which will remain secure in the event of the original copy being destroyed.

Media Disposal
All hardcopy media containing sensitive data is disposed of in accordance with the School's policy for disposal of sensitive data.

All magnetic data is destroyed if the equipment is to be disposed of. Where the equipment is to be recycled the magnetic data is reformatted or checked with specific software to clear the data. Where a third party contractor is used to clear data, a legal disclaimer is required.

Security of Electronic Mail
Email may be used for personal use provided it falls within the guidance defined as 'acceptable use' within the 'good practice guide'.

A separate policy on electronic communications exists.

System Access Controls
User Access Management
No member of staff or student is allowed access to the network without permission being given by HR.

System access rights are withdrawn by the Network Manager as follows:

- For students leaving in the Fifth Form, their accounts are retained until after GCSE results and then system access rights are withdrawn;
- For the Upper Sixth, it is until the end of the Michaelmas term in the next academic year;
- For staff leaving in the Summer Term, their accounts are retained until the end of their contract (31st Aug);
- For students and staff leaving at other times the period of time the account is retained until system access rights are withdrawn is negotiated.

User Password Management
No individual should be given access to a live system unless properly trained. All new staff and students should be provided adequate training in the systems they will require access to.

All new staff and students should be made aware of their security responsibilities.

Users should keep their passwords secret and never disclose them to colleagues. It is a breach of this policy for users to share passwords or sign in other users and can lead to disciplinary action.

All users should change their passwords periodically.

Passwords are not displayed when entering them.

Users who forget their passwords are instructed to contact ICT Support.

ICT Support will verify the validity of the request before issuing a new password. The identity of the individual is always checked before issuing a revised password.

The network maintains a record of previous user passwords. This prevents users immediately reusing a previous password.

User Responsibilities
Staff and students are advices of good password practices:

- Keep passwords confidential;
- Avoid keeping a paper record of passwords;
- Change passwords wherever there is any potential compromise in security;
- Select passwords with a minimum of six digits;
- Avoid basing passwords on potentially guessable formats;
- Change passwords regularly.

Users are instructed not to leave equipment logged on and unattended. Users should ensure that they are logged off systems and sessions.

Login Procedure
Users accessing the network must comply with the all ICT Policies. Prior to logging on users may be prompted with a display notice warning users that 'the computer must only be used by authorised personnel'.

All users should be prompted for a username and password. No user should access the system without using their own user ID.

Application Access Control
The Network Manager and Director of ICT define access and use of application systems.

All unnecessary system utilities are disabled during installation.

All application systems should provide adequate audit trails of transactions.

Systems Development and Maintenance
New Projects
New systems should follow a formal feasibility study of the options prior to selection.

All projects for new systems should consider the security requirements of the system to safeguard the confidentiality, integrity and availability of the information assets. This should be considered during the feasibility stage of the project. Consideration should include:

- Control of access to information;
- Segregation of duties;
- Access to audit trail;
- Verification of critical data;
- Compliance with legislative requirements;
- Backup procedures;
- Recovery procedures;
- Ease of use
- Data Protection and Privacy

Change Control Procedures
Any change to systems, files and data, should be undertaken in a controlled manner. All changes should be documented and tested prior to implementation.

Business Continuity Planning
The Network Manager has identified and maintains a record of business critical systems and processes.

The Director of ICT will periodically review potential risks and their impact on the School. The Network Manager and Director of ICT have identified responsibilities and procedures to follow in the event of disasters for specific servers and systems. Documentation of these procedures and processes are kept on file.

Procedures are tested and reviewed regularly.

Author: GJM
Approval date by Governors: July 2018
Review Date: July 2019