ICT Policy

SUTTON VALENCE SCHOOL

This Policy applies to Sutton Valence School (including as the context requires, the Little Lambs Nursery, the Pre-Preparatory School, Preparatory School and Senior School).

The following policies are in place at Sutton Valence School. These policies cover both students and employees of the School.

The policies included in this document are:

- PC and Laptop Security Policy
- Internet Policy
- Email Policy

(Please note - throughout this document "authorised staff" are defined as those members of staff whom the Director of ICT or the Headmaster have agreed have sufficient authority to interrogate the email system, internet monitoring system, camera footage and view individual results as detailed herein; PC refers to any computer system including laptops)

Sutton Valence School PC and Laptop Security Policy

Objectives
To ensure that the integrity and confidentiality of information, IT systems, IT equipment and IT networks within Sutton Valence School are protected in line with the School's requirements and best practice.

To ensure that all students/employees/governors who use or have access to School information via a School PC understand their responsibilities in relation to the ownership, use and security of that information.

Physical Security of PC equipment

- In order to prevent unauthorised access, damage and interference to IT services, all workstations and related equipment must be secured, so far as is reasonably practicable, against theft and unauthorised use. For example, the use of security cables will help to deter casual theft;
- Cameras are used in areas where IT equipment is located. The cameras images from the cameras are stored on the server and will only be viewed by those authorised when they suspect misbehaviour to have occurred;
- When travelling, portable computers are particularly vulnerable to theft, loss or unauthorised access. They should, therefore, always be carried as hand luggage and must not be left unattended in public places. When travelling by car, laptops, etc should be kept in the boot of the car and should never be left in an unattended vehicle. Where portable workstations are equipped with a form of access protection, (for example, a password or encryption system) this should always be engaged whilst the computer is in transit or is not in use;
- Any loss, theft or damage must be reported immediately to the Network Manager and to the Director of ICT.

Ownership of/Access to information

- Any School-related information which you have created or to which you have been granted access on your PC is your responsibility to protect and remains confidential to the School;
- Personal passwords must not be disclosed or shared for **any reason whatsoever**. It is an offence under the Computer Misuse Act 1990 to disclose your password or access another person's account even with their permission. There is a large element of responsibility placed on the student's and or employee's shoulders regarding this point. Good password practice must be at all times considered. If you believe another student or employee knows your password you must change it immediately. If you are in anyway unsure, or do not know how to do this you must speak to the Network Manager without delay;
- If workgroup passwords are used, these must be maintained solely by the members of the work group;
- Computer systems must not be left logged in and unattended. wherever possible, personal password re-entry should be employed;
- If you are leaving the School, access to all applications will cease at the appropriate time
- Specific breaches of confidentiality, whether within Sutton Valence School or outside the School will be regarded as serious misconduct which **will result** in disciplinary action being taken.

Computer Virus Protection

- Computer viruses pose a threat to the systems of the School. It is, therefore, vital that all computer users adhere closely to any anti-virus procedures and measures issued by the systems department;
- An authorised virus checker must be installed on all equipment before it is connected in any way to the school network. This must not be tampered with and any problems should be reported immediately to ICT Support;
- An authorised virus checker has been installed on all workstations. This must not be tampered with and any problems should be reported immediately to the Network Manager. If you are unsure whether your workstation has a virus checker, you should contact the systems department;
- All acquired data and software should be tested using an authorised virus checker before it is loaded and used. This includes software which may have been obtained through approved supply processes, vendor bulletin boards, other academic networks, the Internet and other public sources;
- Microsoft, from time to time, release operating system updates to protect against virus infection. The Network Manager will inform you when such updates need to be loaded on to your equipment;
- If you discover, or suspect, that your device has been infected by a virus, you should take the following steps:
    a. Note down the symptoms and any messages appearing on the screen;
    b. Stop using the computer and, where appropriate, isolate it from the network (by logging out or, in a worst case scenario, removing the network cable from the device);
    c. Report the incident to ICT Support immediately;
    d. Ensure that any disks being used are not transferred to other computers;
    e. Do not, under any circumstances, attempt to remove the suspected software. Prompt corrective action will be carried out by appropriately trained and experienced staff.

Location/Saving of Electronic Information

- Files should only be saved on school owned devices, no files should be saved on non-School owned devices or online areas that have not been provided by the School;
- Access to online areas, such as OneDrive are provided to all account holders to save and work on files without the need to save them locally on non-School owned devices;

If you know or suspect that a computer system is infected with a virus, you must not use it or allow other people to use it.

Use of Unauthorised Software

- Authorised software only must be used on all School equipment. The reasons for this are:
    a. To safeguard against potential virus risks;
    b. To ensure no breaches of software licence regulations;
    c. Please remember that, under copyright law, persons involved in any illegal reproduction of software will be liable for serious penalties, which can include fines and/or imprisonment;
- Software is authorised only if it is licensed and purchased by the School in accordance with the standards and work practices agreed specifically by SMT and the DICT;
- No unauthorised copying of business or home software programs is permitted.

Making, acquiring or using unauthorised software will be regarded as serious misconduct which may result in disciplinary action being taken. This policy, along with all other aspects of the Computer Misuse Act 1990, will be strictly enforced.

Reporting Incidents

An IT security incident is an event or situation that has, or may have, the ability to compromise the confidentiality, integrity or availability of Sutton Valence School information or its information systems.

Such events may include the intrusion of a hacker into the network, the loss or theft of any computer or telecommunications equipment or casual browsing by unauthorised users.

Students, governors and or employees must report promptly any actual or suspected incidents to the systems department.

Sutton Valence School Internet and Email Policy

Introduction

The Internet is used within Sutton Valence School to facilitate School-related communications and transactions and as a resource to support the goals and objectives of the School and its departments. To this end, the School maintains reliable, cost effective connections to the Internet.

The School may access, audit and monitor the email system at any time in accordance with the SVS Electronic Communications Policy. The purpose of such monitoring is to ensure that the Email system is being used in a responsible manner and that there are no breaches of School policy. This is in order to ensure that the integrity of the IT networks within the Sutton Valence School is protected in line with the School's requirements and best practice.

In carrying out any form of monitoring, Sutton Valence School will ensure full compliance with

all relevant legislation including GDPR, the Human Rights Act 1998 and the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000.

Automated monitoring of all email is carried out on an on-going basis. However, the monitoring of the content of individual emails by authorised ICT staff will be carried out only if it has been established that there is a specific issue/need.

The methods used to carry out any such non-automated monitoring will be proportionate and not unduly intrusive into an individual's privacy.

The purpose of this policy is to outline your responsibilities when you are using the internet and email and to explain the procedures which have been put in place to enable you to use the Internet as a safe and effective tool.

The policy is intended to make users aware of the risks, provide guidelines regarding proper usage, and inform users of the School's rules and procedures regarding use of the Internet and Email.

Access to the Internet and Email

- Sutton Valence School has established a base level of internet connectivity. This base level includes email and web browser access for authorised users to access the internet;
- Authorised email users may use email to communicate with other staff, governors and pupils within the School and have access to the internet for sending and receiving email outside of the School;
- Every authorised user with a web browser has the ability to access sites which have been agreed by the School as having value. Access to these sites is available only from those PCs which are equipped with a web browser;
- If School email has been configured on a personal device then the user is granting the School, under certain circumstances, such as, for example theft or loss of device and with the permission of the Headmaster or Data Compliance Officer, the authority to remotely wipe the device to protect the School's data (where possible this will be done in consultation with the user);
- Certain staff and pupils may need broad access to a wide range of internet web sites. These individuals should direct their requests to their housemaster/manager and systems department in order to obtain the appropriate authorisation and access.

User Responsibilities

As with any other communications tool provided by the School (such as telephones, fax and mail), the internet must be used in a responsible manner consistent with the School's standards of conduct.

- Only authorised users may use the internet and email system;
- Authorised users must ensure they are familiar with this policy and adhere to it whenever they access the internet and email;
- All email is transferred via an internet gateway. Any email which is transferred via the internet should be treated as insecure unless it is suitably encrypted. Sensitive or School confidential information should therefore not be sent in this way;
- As an authorised user, you are responsible for the security of your internet and email account password and any communications which are sent via your account;

- The internet and email system are to be used for Sutton Valence School's business purposes only. The internet facilities may be used for personal, private, or non-School related purposes only with permission of authorised personnel;
- You must only use the email provided by the School for School-related business and must not forward school emails to a personal email account or reply from a personal email account;
- You are responsible for reporting, to your head of house and/or ICT Support, any misuse of the internet or email system, or breach of any of the guidelines outlined in this policy.

Disciplinary Action

- Any member of staff found to be misusing the internet or any part of this policy may be subject to the School's disciplinary procedures and or the cancellation of access to the systems or parts thereof.
- Failure to follow the guidelines laid down in this policy may, in certain circumstances, put both the School and individual users at risk for legal liabilities and prosecution;
- The School assumes no responsibility for any legal damages resulting from your use and/or misuse of the internet or email.

Prohibited Conduct

Users of the internet and email system should adhere to the School's normal communication standards and not use this system for sending or receiving inappropriate messages or materials which are against School policies. Examples of inappropriate internet and email usage include, but are not limited to, the following types of conduct, which are expressly prohibited by this policy:

Illegal or Wrongful Conduct

Engaging in any fraudulent, illegal or wrongful conduct or activities.

Copyright Infringement

Copying, reproducing, printing, transmitting, distributing, or otherwise disseminating copyrighted materials (including text, graphics, photographs, computer software, etc.) in breach of copyright laws, or other intellectual property laws, unless you have obtained written permission, or licensing agreements, or these materials have been made freely available by the owners, or the use qualifies as permitted "fair use" under the copyright laws. (The fact that a particular work does not have a copyright notice, or is accessible on the internet, does not mean that it is not protected by copyright or that it is publicly available. Please contact the Director of ICT if you are in any doubt.)

Violations of Trademarks and Other Intellectual Property Rights

Using without authorisation trademarks and/or other intellectual property rights (i.e. patents, trade secrets. etc.) of third parties in ways which infringe such rights and which are in breach of intellectual property laws or related rights.

Use of software or hardware to circumvent the schools filtering system

Using software on any device including but not limited to VPNs and proxy avoidance applications or any hardware device that may attempt to alter the route of internet traffic.

Confidential Information

Sending, receiving, printing or otherwise disseminating confidential, trade secret, proprietary, privileged, or other sensitive information without prior authorisation and reasonable security measures in place (e.g. encryption). (You should never send anything over the internet which

is truly confidential, trade secret, proprietary, privileged or otherwise sensitive, since third parties may be able to gain access. When sending personal sensitive information, the information should be password protected and the password transmitted to the receiver via an alternative means of communication.

Objectionable Messages and Materials
Sending, accessing, downloading, copying, displaying or otherwise disseminating messages or materials which contain offensive or objectionable matter, including but not limited to material which is (or which could be construed as):

- Being abusive, profane, vulgar, threatening, harassing, discriminatory, disparaging, defamatory, false or libellous;
- containing sexual implications, racial or ethnic slurs, gender-specific;
- comments or comments which offensively address someone's sex, sexual orientation, religious or political beliefs, nationality, disability or other classifications protected by legislation;
- containing pornographic or other sexually explicit or obscene messages, images, or materials of any kind;
- containing other non-School like materials, or inappropriate or offensive communications.

Unauthorised Access
Accessing, or attempting to access, restricted or proprietary third party files, communications, web sites or other remote systems ("restricted areas") without permission from the owners of such restricted areas.

Risk of Viruses
Not following School procedures, or not taking precautions for downloading, screening or avoiding computer software viruses coming from outside or unfamiliar sources over the Internet, or coming from incoming email, as well as from any disks/memory sticks containing files used on the internal network.

Unsolicited Email, or Solicitations etc.
Sending unsolicited email, chain letters and other forms of mass mailings and solicitations which are not approved. This includes communications for personal, political and other non-business purposes.

Personal Opinions Without Appropriate Disclaimers
Transmitting one's own personal opinions to Internet public groups (i.e. forums, news groups, bulletin boards, discussion group, or other Usenet groups) without including an appropriate disclaimer that the views expressed are your own, unless you have confirmed that they represent an official School position.

Internet Communication and Email Usage

Privacy
Staff and pupils should be aware that the School's standard internet and email system and web browser facilities are not designed for sending or receiving private or confidential electronic communications.

When using email to communicate with parents, iSAMS should be used or, if this is not possible, BCC should be used to protect the email addresses of the recipients.

All internet messages should be considered to be readily accessible to the general public. The system should not, therefore, be used for any communication which the sender intends only the original addressee(s) to read.

Potential Permanence of Email
The use of email creates a record which may be permanent. Messages may exist on backup tapes or otherwise be retrievable from the system for undefined periods of time. Accordingly, only messages suitable for long-term storage should be sent.

Electronic Signature
No information which you send or receive over the internet is anonymous. Any information sent over the School's internet connections contain an "electronic signature". Any messages which contain the types of prohibited statements or transmissions referred to in the "Prohibited Conduct" section above are forbidden.

All internet and email correspondence should be treated as though it is being sent on a School letterhead and as though anything which is sent or received may be accessible by others. Whenever you send email, your name and user id are included in each mail message. You are responsible for all email originating from your user id.

Retention or Deletion of Information
With respect to messages, documents or other information which users have saved on the School's internet or email system, (or which they have not deleted from the system), the School reserves the right to remove such messages, documents or other information from the system on a monthly basis or within such reasonable time period as may be determined by the School.

Users of the system should periodically delete email contents or save them either by archiving such contents to hard disks, or printing and filing hard copies of such information.

Internet or email contents which are not saved by the user, or which are deleted or erased by the user, may remain stored in the School's computer system for a period of time to be determined by the School and may be accessed by the School during such time.

In the event of cessation or termination of a student’s education/employee's employment by the School, or of a non-employee's business relationship with the School, all access to the School's access to the internet and email system will be terminated. Internet and email messages are subject to discovery order, or disclosure orders, or disclosure, in litigation matters and in other judicial or administrative procedures.

Email and Internet Monitoring
Staff and pupils with authorisation to use the internet and email system should note that the School may, but is not obligated to, access, audit, and monitor its email and internet system as well as the contents of email messages and other information contained on the system.

The School reserves the right and intends to periodically monitor, audit, review and disclose, as necessary, internet and email communications and messages. Your proper use of the system will

help avoid inappropriate disclosure of proprietary, confidential, and other sensitive information, prevent unexpected liability and ensure the security of our internet and email system.

System administrators at the destination system and intermediate service providers may monitor and review computer communications transmitted on a random basis to verify appropriate use and compliance with this policy. All monitoring will be done in accordance with school policy.

By using the School's internet and email system, users consent to the School's right to:

1. Access, audit, and monitor the contents of email messages and internet information in line with the School Electronic Communications Policy.

2. Use, disclose, or delete such contents or information, with or without further notice.

Nothing in this section gives any unauthorised staff and pupils the right to access anybody else's email messages, without the prior approval of the Director of ICT or Headmaster and the third party involved.

Process of Monitoring

- The monitoring of the actual content of emails by authorised ICT staff will be carried out on a random basis;
- In the first instance, all Email traffic is monitored using an automated content checking utility which automatically 'reads' every email and checks the content for key words or content;
- If the content checker discovers key words or content, then the email will not be delivered to the intended recipient but will be placed automatically into a holding account;
- Once in the holding account, the email will be physically checked by one of the ICT technicians in order to determine why the email has been blocked;
- If the message is clearly School-related it will normally be released within 30 minutes of being detained. Please note that there is an additional delivery delay outside the control of the School as the message is sent through the public internet;
- If the message is considered non-School related, then it will remain blocked

Automated Content Checker

The content checker will block emails which contain content that may be contentious. Such content will fall, broadly, under two headings:

- Attachments, images and sound files. (Whether alone or embedded into a document). For example (but not exclusively):
  *.jpg, *.gif. *.avi, *.bmp, *.cgm, *.tif, *.exe, *.cmd, *.com, *.zip, *.wav
- Inappropriate language
  Language which may be considered to be profane, vulgar or offensive will be detected and may lead to the email to be blocked. It should be noted that the system may be 'triggered' by one key word only, by a number of different words used in succession, or by one word being repeated to excess.

Support

a) Individuals and departments with specific electronic commerce requirements beyond standard internet, email and web browser access must be authorised by the Network Manager/Director of ICT who will then take the appropriate action;

b) No network connectivity to the internet or any registration of internet names and addresses is to be conducted by individuals or departments outside the systems department, without the approval of the Director of ICT, Network Manager or Headmaster.

Computer Virus Protection
The internet gateway is secured with a virus scanner and also with a content checking utility.

The virus scanner is an automated system which ensures that known computer viruses do not enter or leave the Sutton Valence School email system by dissecting each email and ensuring that it does not contain any virus infection. It is present for the protection of the School's systems; however pupils/employees still carry responsibility for ensuring that viruses are not introduced into the School via any means. If a pupil/member of staff is aware that they have received an email which is infected it should not be opened and advice from ICT Support should be sought immediately.

Author: Mr Glen Millbery
Policy Date: September 2023
Approval Date by Governors: November 2023
Review Date: September 2024