SIR THOMAS RICH'S
Information and Communication Technology Policy

Date reviewed: May 2018
Status: Non-statutory
Responsibility: It is the responsibility of the Governors' Evaluation and Curriculum Committee to monitor the implementation of the policy and to review it at regular intervals. The day-to-day management of ICT is undertaken by the Network Manager, who reports to the SMT.

Contents:

1. Introduction

ICT plays a vital role in a successful school. It supports teachers in delivering interesting and effective lessons, offers pupils enriched learning experiences, whilst promoting initiative and independent learning. The internet enables rapid access to information from a wide range of people, communities and cultures. The technological revolution has brought many changes to the way in which information is shared, the majority of which are advantageous.

However, the School is aware that it has the potential for harm. The ICT policy aims to ensure that:

- Pupils are well equipped with the necessary skills to use ICT effectively across the curriculum and beyond and are aware of the limitations of ICT as well as the advantages.
- All users are aware of how to use ICT responsibly and safely.
- Measures are in place to safeguard pupils and protect them from extremist and terrorist material. *See the School's Child Protection and Safeguarding Children Policy and Preventing Extremism and Radicalisation Policy.*
- All information held electronically is secure, and the School complies fully with the Data Protection Act.

2. ICT Facilities

In addition to computers in the Learning Resource Centre and other dedicated study areas, there are three dedicated computer suites for general use and a Design and Technology and a Specialist Languages suite. All classrooms have a projector and many an interactive whiteboard.
Printing carried out by pupils is constantly monitored. Printing costs incurred by teachers are met from departmental budgets.

The School has wireless internet connection (Wi-Fi), giving laptop users access to login via Remote Learning. The content is filtered as for a regular school PC. Internet access via a mobile phone is not permitted. If a pupil or member of staff wishes to connect a personal device to the internet, they connect to the appropriate wireless network and login using their credentials. If a visitor wishes to connect to the internet, voucher codes are available from reception, or are provided to staff to distribute for larger events.

The School also provides a virtual learning environment which can be accessed both in school and from home. This is used to provide information and support for students such as past examination papers and other work.

3. The Provision of ICT and Computing within the curriculum

Most boys come to the School with a solid background in basic ICT skills and many with a level of competence that is much higher. Dedicated computing lessons are timetabled in Year 7 and Year 8. In Year 9 Computing is scheduled as part of a 'roundabout' of subjects.

Computer Science is taught as a subject at GCSE.

The curriculum for Year 7 reviews basic ICT skills and introduces pupils to the workings of computers and networks. Year 7 lessons also include an introduction to programming skills. Year 8 students follow a course designed to improve their understanding of computing systems and to further develop and encourage the skills they require for programming computers. Year 9 students undertake an introduction to more traditional programming. The Computing courses set out to develop the skills that students will need to allow them to code programmes and understand how programmes work.

Alongside these skills, the ICT department teaches the responsibility and security necessary for today's online world, the importance of observing copyright and licensing laws and the need to validate the accuracy of information.

For further information contact Mr P. Johnson, Head of Computing pwj@strs.org.uk

4. E-Safety

The School understands the responsibility to educate its pupils on e-safety issues to ensure they remain both safe and legal, when using the internet and related technologies. It does this through ICT lessons, the wider curriculum and effective monitoring and filtering.

The responsibility for e-safety lies with staff, who receive training on e-safety, pupils and parents.

I. Monitoring and Filtering

The School provides a filtered internet service and has appropriate levels of monitoring in place to protect children from harmful and inappropriate material. e.g. material which is illegal and/ or relates to Bullying, Discrimination, Child Sexual Exploitation, Drugs/ Substance Abuse, Extremism, Pornography, Self-harm, Violence or Suicide. The School's Internet Provider is an IWF member and blocks, amongst other inappropriate material, access to CAIC (Child Abuse Images and content). Pupils are supervised, where possible, when using the internet. Access to the internet is logged and pupil access monitored regularly by the ICT team for any misuse. The School's filtering system gives log file information that details and attributes websites access and search term usage against individuals. The system is multi-lingual and tackles malware/hacking issues and piracy and copyright theft.

II. Responsibilities

Senior Management

The Senior Management team has responsibility for ensuring that ICT in the School is properly managed, that e-safety guidelines are observed and all information held electronically is secure.

Network Manager and support team

The Network Manager, currently Mr M. Hopton, and his team, are responsible for ensuring that:

- the ICT infrastructure is secure and not open to abuse.
- the School meets the e-safety technical requirements.
- access to the School's networks is only possible through the control of passwords.
- the School's filtering policy is applied and updated on a regular basis.
- the School's network is regularly monitored so that incidents of misuse can be detected.
- monitoring software systems are implemented and updated.
- guidelines for the safe disposal of redundant ICT equipment are followed.
- a file is kept of all licences and other documentation relating to hardware and software.
- internal audits of both hardware and software are regularly carried out to check full compliance with licence agreements.

Teachers and support staff
Staff are responsible for ensuring that they observe e-safety measures and adhere to the ICT Acceptable Use Policy for staff. They should also check that pupils follow the Acceptable Use Policy for pupils.

Pupils
Pupils are responsible for working in compliance with the ICT Acceptable Use Policy for pupils.

Parents
Parents should be aware of the ICT Acceptable Use Policy for pupils. It is their responsibility to monitor their child's use of the internet at home.

III. ICT Acceptable Use Policy for Staff

- The ICT facilities should only be used as required by work duties.
- Users should ensure that critical information is not stored solely within the School's computer system. The ICT team does not guarantee backups. If necessary, documents must be password protected.
- Staff must comply with the School's Data Protection Policy when handling personal data.
- Data stored on the ICT systems is the property of the School and may be subject to Freedom of Information requests.
- Staff should lock/log off their workstations before leaving them.
- Approval of new software must be gained from the ICT department before software is purchased.
- Staff should monitor ICT activity in lessons, enforce the need for pupils to avoid plagiarism and guide pupils doing research to sites which have been checked as suitable.
- Any suspected misuse should be reported to Senior Management.

N.B. Staff user accounts are accessible by the ICT department.

Staff are **not permitted to:**

- use the ICT facilities for commercial and financial gain.
- re-locate, take off-site or otherwise interfere with the ICT facilities without the authorisation of the ICT department.
- use or attempt to use someone else's user account. All users are issued with a unique user account and password. The password must be changed at regular intervals. The ICT department issues reminders. It must never be disclosed.
- allow anyone else to use their account, even with supervision.
- use ICT facilities to access, download, send, receive, view or display:
  - material which is illegal.
  - remarks which could constitute bullying or harassment (including on grounds of sex, race, age, religious belief, sexual orientation, gender reassignment or disability).
  - material or comments which promote discrimination, violence, racial or religious hatred, drugs and substance abuse.
  - negative comments about other persons or organisations which may adversely affect the reputation of the organisation or person regardless of whether they are true or false.
  - sexually explicit material.
- use or attempt to use the School's ICT facilities to undertake any form of piracy e.g. infringement of software licences. Staff must observe copyright provisions and may not copy, download or distribute any material when it is illegal to do so. If permission is unclear and cannot be obtained the material may not be used.
- gamble online.
- access internet-based chat sites.

Laptops
If a laptop computer is loaned to a member of staff he/she is responsible for its safekeeping and appropriate use. The laptop remains the property of the School and any insurance cover is the responsibility of the School, when the laptop is on school grounds. The School cannot be held accountable for loss as the result of theft or otherwise when off-site. The Network Manager is responsible for ensuring that anti-virus software is installed, and all software on the laptop is covered by any licence requirements.

Appropriate use of email

All staff are provided with their own email account for school purposes. Staff are responsible for the content of all emails sent and received by them. The sending of offensive emails is forbidden. Email attachments should only be opened if they come from a known source.

Electronic communication with pupils

- Emails to students should be restricted to school matters. Staff should not use their personal email accounts.
- Staff should use the school mobile to communicate with students while on trips. They should not normally give students their personal mobile number or home number without the permission of the Headmaster.
- Any digital communication between staff and pupils must be professional in tone and content.
- Personal Social Networking Sites must not be used for communication with current students. If staff have a profile on a social networking site, they must ensure that it is private and not accessible by pupils. Staff may not post negative comments or inappropriate images relating to the School on their profile.
- The Headmaster may authorise the use of a social networking sites for communication with students on official school business.

IV. ICT Acceptable Use Policy for pupils

Sir Thomas Rich's believes in the educational value of providing access to ICT to support the curriculum. The use of the internet is a privilege and inappropriate use may result in that privilege being withdrawn. Pupils should report any misuse of the network to a member of staff. All use of the internet by pupils can be monitored and logged and made available to staff.

Pupils are expected to abide by the following rules:

- Use the School ICT system only for school purposes.
- Be polite and use appropriate language in all communications. The sending or receiving of any email, which contains any inappropriate material, is strictly forbidden. It is also forbidden to send large volume emails (spamming)
- Do not reveal any personal information to anyone, especially the home address or personal telephone of yourself and any other students.
- All use of the system must be under your own username and password unless specifically directed by a member of staff. Do not reveal your password to anyone. If you think someone has obtained your password, contact a member of the ICT department. Anyone disclosing passwords may have their access denied.
- Do not use the network in any way which would disrupt use of the service by others.
- It is strictly forbidden to use the School's internet services for ordering goods or services regardless of their nature or to subscribe to any newsletter, catalogue or other form of correspondence.
- Do not eat or drink near any machine.
- The playing of online games is forbidden, unless authorised by a member of staff.
- Do not connect personal and non-authorised devices to the School's network.
- Pupils may not access social sites e.g. Facebook on the School system.
- Do not download files such as executables, movies or music files or run any programme which has not been authorised.
- Ensure that online activity both inside and outside school does not cause distress to others and bring the School into disrepute.
- Do not deliberately browse, download, upload or forward material that could be considered offensive or is illegal.
- Respect the privacy of others' work on line.
- Do not attempt to bypass the internet filtering system.
- Observe copyright regulations and avoid plagiarism.
- Follow School policies on the use of mobile phones and other digital appliances.

Pupils **must not:**

- access inappropriate material either at school or at home when engaged in school work.
- take photographs or videos of members of the School community, unless at the request of a member of staff.
- be party to cyber-bullying.

Sanctions

Pupils are responsible for their own behaviour when using the internet. Any person breaking the rules may be banned from the computer rooms at lunchtimes, have their access limited to computers that are easily monitored or receive a detention. For very serious offences Senior Management will issue appropriate sanctions. Where a pupil has behaved unlawfully, criminal proceedings may ensue.

V. Visitors

If a visitor wishes to use the ICT facilities, he/she should speak to the Network Manager who will make the necessary arrangements. Visitors should follow either the ICT Acceptable Use Policy for staff or pupils, as appropriate.

VI. Photographs and videos

On a pupil's entry to the School all parents are asked to give permission to photograph or video their child for educational purposes. This consent form is considered valid for the entire period the pupil attends the School. Images might feature on the School website, in a School prospectus, display material in the School or press releases. Pupils' names will not be published alongside their image, unless the consent of both the Headmaster and parents has been obtained. Images of pupils might also be used in the classroom for learning and teaching purposes. A list of those pupils for whom consent has not been given is kept securely in the office of the Headmaster's PA.

Staff are advised to use school equipment to take images. Where this is not possible images should be transferred as soon as possible to the School network and deleted from personal equipment.

The School uses CCTV for security and safety. Only the Headmaster, ICT team or teachers designated by them have access to the images. Images will be deleted within 60 days.

5. Data Security

The School takes its duty to keep data secure very seriously.

Access by pupils and staff to all types of data held on the teaching and administration networks is only permitted through the controlled issue of passwords. The servers are sited in locked rooms. Pupil records are kept on SIMS on the School's administrative network. A full programme of data back-up procedures is implemented twice daily. Users can use "shadow copies" to retrieve versioned data for up to 30 days, and ICT staff can further restore back another 90 days.

All users must have regard to the importance of keeping data secure and minimise the risk of loss. Pupils' personal data should not, if possible, be saved on laptops. Where this is unavoidable, it should be transferred as early as possible to a secure location on the School's network and then deleted. Users should be particularly vigilant about logging off at the end of a session when personal data has been accessed. Personal data must not be stored on removable devices other than for transferring data between computer systems.

All parents are offered access to "Parent Gateway" where they can view data held by the School about their child. This includes attendance, published reports, SEND (Special education needs and disabilities), medical notes and home address. If the child's parents live at different addresses, both parents will be offered the service, providing the parent who lives at the child's registered home address confirms in writing that there is no reason why the absent parent should not have access. Any reason to withhold access must be supported by appropriate evidence. e.g. court order.

Appendix 1

Staff Personal Device Policy

1. **USB Storage**

USB memory devices are permitted where necessary but these must be authorised and encrypted by the school in order to work on the school network. Use of such devices is discouraged as they can easily be lost or misplaced. Under no circumstances should personal data be saved to an unencrypted USB memory device.

2. **Working Remotely**

Staff may use the school's Remote Access system to work from home or elsewhere, including working on files that include personal data. However, staff should ensure:

- their device is never left unattended while logged into Remote Access
- that they use an internet connection which they know to be secure (not public wifi) using a device which they own
- that they take reasonable care to protect personal data against being viewed by unauthorised individuals
- that they take precaution to ensure the security of their login credentials and regularly install updates on any device accessing remote access
- that any files which contain personal data remain on the school servers and are not copied to their local machine
- that any files which contain personal data are not printed when using Remote Access

3. **Photographs**

Staff may take photographs of pupils involved in school activities that on their personal devices provided the following guidelines are met:

- photographs are transferred to school servers as soon as is feasibly possible and then deleted from the personal device
- photographs are not uploaded to cloud services (staff should check that automatic back up to these services is turned off)
- the circumstances under which the photographs are taken are those in which a pupil may expect to be photographed (sporting event, drama event, trip activity, whole class activity)

Staff email

Staff may use personal devices for notification of school emails provided that the following guidelines are met:

- devices are protected by a password, a PIN or biometric security and device updates are installed regularly
- any attachments which contain personal data should not be saved to the local storage of the device – for most devices this will mean that such attachments should not be opened on a personal device
- staff should not forward any emails which contain personal data to any email address which is not an strs.org.uk email
- staff should not use their school email address for signing up to non-school related services
- personal email addresses should not be used for any school business, activities or data

Due to the confidential nature of some emails, use of any unsecured device for staff emails is prohibited.

Appendix 2

CCTV Policy

1. Introduction

This policy forms part of the School's ICT Policy and will be reviewed along with it. The purpose of this Policy is to regulate the management, operation and use of the CCTV system at Sir Thomas Rich's School (the School).

The system comprises of around 75 cameras located in and around the school site. All cameras are managed by the ICT department and images are only available to selected senior staff.

This Policy follows Data Protection Act guidelines.

2. Objectives of the CCTV system

- To protect pupils, staff and visitors.
- To increase personal safety and reduce the fear of crime.
- To protect the school buildings and assets.
- Without prejudice, to protect the personal property of pupils, staff and visitors.
- To support the police in preventing and detecting crime.
- To assist in identifying, apprehending and prosecuting offenders.
- To assist in managing the school.

3. Statement of Intent

The CCTV system will seek to comply with the requirements both current Data Protection Law and the ICO Code of Practice.

The school will treat the system, all information, documents and recordings as data protected under the law.

Cameras will be used to monitor activities within the school and its grounds to identify actual or anticipated criminal activity. It will be used for the purpose of securing the safety and wellbeing of the pupils, staff and visitors.

The system has been designed to deny observation on adjacent private property.

Materials or knowledge secured as a result of CCTV will not be used for any commercial purpose and images will only be released to the media for use in the investigation of a specific crime with the written authority of the police.

The planning and design has endeavoured to ensure that the system will give maximum effectiveness and efficiency but it is not possible to guarantee that the system will cover or detect every single incident taking place in the areas of coverage.

Warning signs, as required by the Code of Practice of the Information Commissioner will be clearly visible on the site.

4. System Management

The system will be administered and managed by the School who will act as the Data Controller, in accordance with the principles and objectives expressed in the policy.

The day-to-day management will be the responsibility of the Network Manager who will act as the System Manager.

The system and the data collected will only be available to selected members of senior staff

The CCTV system will be operated 24 hours each day, every day of the year.

The System Manager and his team will regularly check and confirm the efficiency of the system and in particular that the equipment is properly recording and that cameras are functional.

The System Manager must satisfy themselves of the identity of any person wishing to view images or access the system and the legitimacy of the request. Where any doubt exists access will be refused.

Images will be retained for no longer than 30 days except where the images form part of an ongoing internal or external review or investigation; in the latter case the images will be retained for the duration of the investigation and any subsequent appeal.

5. Complaints

Any complaints in relation to the school's CCTV system should be addressed to the Headmaster.

6. Subject Access Requests

Data Protection legislation provides Data Subjects (individuals to whom "personal data" relate) with rights relating to data held about themselves, including those obtained by CCTV.

Requests for Data Subject Access should be made in accordance with the School's Data Protection Policy and will need to reference specific dates, times and locations. The CCTV data will be made available for viewing in the presence of an authorised member of staff and will be subject to the protection of the privacy of other individuals.